OVERVIEW OF THE CYBER PROBLEM: A NATION DEPENDENT AND DEALING WITH RISK

HEARING

OF THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH, AND DEVELOPMENT

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 22, 2003

Serial No. 108–13

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

98–312 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, Ranking Member
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
STEVE NASH, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

MAC THORNBERRY, Texas, Chairman

PETE SESSIONS, Texas, Vice Chairman
SHERWOOD BOEHLERT, New York
LAMAR SMITH, Texas
CURT WELDON, Pennsylvania
DAVE CAMP, Michigan
ROBERT W. GOODLATTE, Virginia
PETER KING, New York
JOHN LINDER, Georgia
MARK SOUDER, Indiana
JIM GIBBONS, Nevada
KAY GRANGER, Texas
CHRISTOPHER COX, CALIFORNIA, *ex officio*

ZOE LOFGREN, California
LORETTA SANCHEZ, California
ROBERT E. ANDREWS, New Jersey
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
JIM TURNER, Texas, *ex officio*

CONTENTS

OVERVIEW OF THE CYBER PROBLEM: A NATION DEPENDENT AND DEALING WITH RISK

Wednesday, June 25, 2003

U.S.HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE,
AND RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 11:30 a.m., in room 345, Cannon House Office Building, Hon. Mac Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Sessions, Boehlert, Smith, Gibbons, Lofgren, Andrews, Jackson-Lee, Christensen, Etheridge, Lucas, Langevin, and Turner [ex officio].

Mr. THORNBERRY. The hearing will come to order. The Subcommittee on Cybersecurity, Science, and Research and Development is meeting today to hear testimony on an Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk. And Ms. Lofgren and I ask unanimous consent that all members be able to submit written opening statements but that oral written statements be waived beyond the Chairman and Ranking Member. Without objection, it is so ordered.

We do have some time constraints on how long we can use this room, so we want to keep our comments to a minimum and get right to it. Let me just say that this subcommittee is charged with a number of homeland security responsibilities. One of the most complex is this issue of cyber security: the online world of computers, networks, information, and the physical and virtual lines that tie it all together. Obviously our country is becoming more and more dependent upon the Internet and information technologies. That growing dependence just as obviously leads to greater vulnerabilities, and part of our job in this subcommittee is to try to get our arms around those issues and see if there are other Federal actions that may need to be taken.

We are pleased to have a distinguished group of witnesses to help us get our arms around those issues today. Before yielding to them, let me yield to the distinguished Ranking Member, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman, and thanks for calling this hearing today. I first want to offer an apology. At noon I am chairing another meeting of the California delegation and so will have to slip out for a while, but I want to assure the panelists that I have read their testimony and look forward to working with them in the future.

I think this is an important hearing to scope out the elements of the challenges that we face, and I hope with regard to the DHS itself, that the witnesses will share their opinions on the newly created Cybersecurity Division, talk about the meetings they have had, if they have had; if you have concerns about the placement of the division within DHS, please share that. Will it have access to the Secretary? Sit buried too deep? I have some skepticism about the DHS plan for cybersecurity. I fear that we are moving too slowly. If you think that is correct, let me know. If my fears are misplaced, I would love to know that as well.

I would also—looking beyond DHS, I would hope that you could enlighten us as to what steps the Federal Government might take to encourage the private sector to make cybersecurity a higher priority. And I would especially like to welcome Bruce Schneier, who I have known for many, many years and thank him for coming all the way out to be a panelist as well as the two other really spectacular witnesses.

So, Mac, it is great working with you, and I look forward to the hearing.

[The information follows:]

PREPARED STATEMENT THE HONORABLE MAC THORNBERRY, A REPRESENTATIVE IN CONGRESS

I want to welcome Members, witnesses, and guests to this hearing. This subcommittee is charged with oversight of several important issues related to homeland security. One of the most complex and least understood resides in the world of "cyberspace"—the on-line world of computers, networks, information, and the physical and virtual lines that tie it all together.

Some have called cyberspace the information super highway. Its roads are becoming more crowded and more dangerous, and today's seat belts and guard rails may not be adequate for the challenges that lie ahead. Unlike our physical highways, however, governments do not own most of the roads, and there is much that we do not know about how to make them safe and secure for everyone to travel.

The steady rise in electronic commerce, e-government, and Americans' everyday reliance on the Internet make it even more important that we better understand the threats, vulnerabilities, risks, and recovery options. Even more importantly, the public and private sectors must establish new partnerships and better ways to jointly establish appropriate rules of the road to promote commerce, protect privacy, and make the Internet safer for all travelers.

We do not yet fully appreciate America's dependency on this borderless, virtual world, but we know it is growing—and it is growing fast. Only 90,000 Americans had Internet access in early 1993 (U.S. Internet Council, Apr. 1999). By 2002, the number of Internet users surpassed 665 million (Computer Industry Almanac, Inc., Dec. 2002).

We don't know how all of the nation's critical infrastructures are linked and dependent upon each other, but we know adversaries, criminals, hackers, and terrorists are trying to figure out how to exploit our weaknesses. We may not fully appreciate the difference between a cyber crime and a cyber attack on our critical infrastructure, but we know the immediate results have cost us billions of dollars in productivity and financial loss. According to the Computer Emergency Response Team at Carnegie Mellon University the number of vulnerabilities have doubled each year for the past five years. According to Chief Security Officer Magazine, nine out of ten Chief Security Officers indicate their companies have been victimized by cyber attacks in the past year. There may come a time when a cyber incident could also cost American lives, especially if there are concurrent attacks on physical and virtual infrastructures.

The Homeland Security Act of 2002 gives the Department of Homeland Security a central role in working with the private sector and with state, local, federal, and international entities to help secure cyberspace. Understanding threats to cyberspace, identifying vulnerabilities that could be exploited, and coordinating response and recovery efforts needed to ensure services are delivered across our critical infrastructure are some of the key functions for the new Department and the areas we

will cover today. A panel of three academic and industry experts will help us understand three foundational issues—cyber threats, vulnerabilities, and response and recovery.

- **Mr. Bruce Schneier** is Founder and Chief Technical Officer, Counterpane Internet Security, Inc., a consulting firm specializing in cryptography and computer security. He will focus on the cyber threats within the nation's critical infrastructure.
- **Mr. Richard Pethia** is Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University. CERT has provided a central response and coordination facility for global information security incident response and countermeasures for cyber threats and vulnerabilities since 1988. He will focus on the vulnerabilities facing the nation's critical information infrastructure.
- **Mr. Alan Paller** is Director of Research, the SANS Institute, a cooperative research organization that delivers cybersecurity education to people who secure and manage important information systems. He will focus on response and recovery by the private sector and government to the threats and vulnerabilities facing the nation's critical information infrastructure.

Their testimony will help us put into perspective the industry, academic, and government partnerships needed to help the Department of Homeland Security perform its mission as it relates to cyberspace. Our ultimate goal is a superhighway that is safe, accessible, fast, and free of unnecessary speed bumps.

Before yielding, I want to thank Eric Fischer and his team from the Congressional Research Service who have again done significant work to help prepare for this hearing. Finally, I want to thank my partner on this subcommittee, Ms. Zoe Lofgren, for her leadership and expertise in these issues. And I would yield to her at this time.

PREPARED OPENING REMARKS OF THE HONORABLE CHRISTOPHER COX, CHAIRMAN, SELECT COMMITTEE ON HOMELAND COMMITTEE

Since May 16th, what was thought to be a Trojan—named Stumbler, that carry potential computer viruses, had been randomly scanning internet connected machines. Private internet security companies, the FBI, and the Department of Homeland Security have been tracking this rogue activity since an employee at a defense contractor notified both the FBI and the CERT Coordination Center. What concerned most experts was the ease with which this "Stumbler" could be reprogrammed to make it more damaging.

The "Perimeter Defense Model" for computer security has been used since the first mainframe operating systems were built. This model is primarily based on the assumption that we need to protect computer systems from the "inside." Based on this underlying assumption, cybersecurity has emphasized "firewalls" and other mechanisms to keep outside attackers from penetrating our computer systems. The continued investigation has revealed that the attacker deliberately planted the "Stumbler", clearly circumventing any internal firewalls.

We need new solutions to prepare for increasingly aggressive attacks on our cyber-information infrastructure. Our society is increasingly interconnected. Our financial institutions, power plants, nuclear facilities, water treatment plants, factories, government agencies, borders, and other critical infrastructure rely upon internet-based technologies for remote monitoring and control of the facilities. While this capability has allowed for amazing advances and improvements in the delivery of services, it also allows for potential access of a cyber-terrorist to each network.

As we begin to look outside established paradigms and partner with the private sector, we have to make securing our information infrastructure an urgent priority. By harnessing the technical resources of the private industry and the intelligence capability of the federal government, we begin a partnership that can prevent, protect, and respond to a Cyberattack.

We lead the world in information technology. The exponential net gain of knowledge over the past decade has led to a pervasive dependence on information and communication systems that affects every aspect of our lives. The good news is the potential this represents to improve the quality of life around the world. But there is also bad news; this growing reliance makes our cyberspace a viable target for terrorists. The very same information technology that has enabled this country to be a leader in the world market can be co-opted by terrorists and used against this country's infrastructure. This type of technology is no longer the exclusive domain of states. Non-state sponsored groups with limited technical capabilities have the capacity to inflict great harm to our safety and economy. A serious attack could potentially cripple our emergency response, health care delivery, transportation, electric grids, and finance systems. A precision attack by a simple virus that would prevent

for just one day our ability to cash a paycheck, prevent stocks from being traded or make a credit card purchase could bring much of our commerce to a halt. Consider the Saphire computer virus. It infected at least 75,000 hosts and caused network outages, cancelled airline flights, interfered with elections, caused ATM machines to fail, and shut down a 9-1-1 call center outside Seattle, which serves 14 fire departments, two police stations, and a community of 164,000 people.

Essentially, every major critical infrastructure in this nation is a public/private partnership and cyberspace is its "nerve center." We can not be successful in securing the vested common interest without a coordinated and focused partnership between the federal government and the private sector. The private sector brings to this partnership the expertise and technical capability. The government, in turn, can provide the intelligence information, set the standards, and provide the corporate incentives to bridge this partnership.

Cyberspace challenges us with some urgency to define the role of the federal government in this partnership to secure our infrastructure and make America safe. For this reason, I established this subcommittee on Cybersecurity—the only such subcommittee in Congress. Cyberspace is indeed a new frontier that the United States must master. This Committee enthusiastically supports the steps that the Department of Homeland Security has taken in establishing the National Cyber Security Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate. Information exchange and cooperation will allow both the government and the private sector to address awareness, training, technological improvements, vulnerability remediation and recovery operations. We will continue to look to enhance the capability of DHS to stand up this office, to coordinate government Cyber programs and to partner with the private sector—all as a matter of the highest priority.

I thank Chairman Thornberry for his leadership of the Subcommittee on Cybersecurity, Science, and Research and Development and I look forward to hearing from our three witnesses this morning.

PREPARED STATEMENT OF THE HONORABLE JIM GIBBONS, A REPRESENTATIVE IN CONGRESS, FROM THE STATE OF NEVADA

Mr. Chairman, I would like to express to you my gratitude for theopportunity to hear from our expert witnesses and for bringing us together to address the issues before us today.

I would also like to thank Mr. Schneier, Mr. Pethia, and Mr. Paller for taking time out of their busy schedules to prepare their testimony and come before us today in an effort to make our country safer.

These gentlemen should be a great help in assisting us in understanding the nature of the challenges before us.

Certainly, the security of our cyber-infrastructure is extremely important to the safety of our country and our economy.

There is no doubt that our economy, the largest and most dynamic in the world, is extremely dependent on our country's cyber-infrastructure, and it needs to be protected with extreme vigilance.

However, I would like to express my concern about our understanding of the nature of the threats to our cyber-infrastructure, and how we are going about addressing these threats.

Unquestionably, an extremely wide variety and high volume of criminal threats to our cyber-infrastructure exist. These threats range from benign computer hacking committed by bored teenagers, to organized criminals stealing and laundering billions of dollars around the world via the internet.

However, while examples of criminal attacks abound, the examples of cyber-terrorism, at this point, are sparse, and this begs the question: Why?

Presently, the internet seems to be an extremely valuable tool to terrorists for the same reason it is an extremely valuable tool to legitimate commercial enterprises and private citizens: it is the supreme medium for communication.

To my knowledge, the only known terrorism-oriented web-launched attack on major infrastructure has occurred in Australia, where the individual responsible dumped sewage into public waterways.

While this certainly provides an example of the damage which can be caused by malicious individuals, it is only a single example, and does not seem to bear witness to the catastrophic cyber terrorism we often hear is at our doorstep.

My intent is not to dismiss the danger that is genuinely posed by our cyber vulnerabilities. It exists and is accepted.

However, it is my great concern that the nature of the threat of cyber-terrorism is being overlooked, and therefore, being addressed improperly.

We cannot properly devise an effective strategy to counter cyber-terrorism if we do not understand the nature of the capabilities of our enemies, and especially if we do not understand the nature of our own vulnerabilities.
I welcome the comments of our witnesses today on the nature of our infrastructure vulnerabilities, and specifically if these vulnerabilities are easily exploitable for mass-disruption attacks.
Further, I welcome comment on the nature of the intellectual and materiel capabilities needed by a terrorist organization to succeed in causing a major internet-based attack on our cyber-infrastructure, and especially our physical infrastructure.
In seeking to understand how best to address the threat of cyber-terrorism, we must begin first by asking the right questions.
This must lead to an understanding of ourselves and our enemies, from which we can craft a successful strategy.
I welcome the candor of our witnesses in addressing these concerns, and thank them in advance.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, I thank you for your efforts in creating this opportunity for this body to hear the testimony of the three panelists today. In our task of gauging the newly developed Department of Homeland Security against the projected needs of our nation, we must begin our evaluation at the most basic levels. Critical infrastructure protection is important to every member of our national and local communities. In order to implement a program of securing cyberspace at a national level, we must follow a course of risk assessment, education, and careful reaction at the local level to protect our schools, hospitals, and rescue facilities. These goals are part of the impetus for the amendments that I offered as to the Department of Homeland Security Appropriations Act and to the Project BioShield Act so that funding mechanisms and the Secretary's discretion contain the control provisions necessary to ensure the proper and effective allocation of resources to the places that have the most urgent needs.

Just as we must ward against the large threats to our critical infrastructure, the small incidents must not be allowed to create a large problem.

In Houston last year, a 21-year-old man was sentenced to three years in prison for a terrorist hoax concerning a plot to attack the opening ceremonies of the 2002 Winter Olympics in Salt Lake City. The Houston resident was sentenced by U.S. District Judge and ordered to pay $5,200 in fines. The Judge told the Defendant that she had sentenced him to three years because he had failed to demonstrate he understood the seriousness of his crime and disruption he had caused to federal agencies and private citizens.

The perpetrator told the FBI in Houston that he had intercepted e-mails between two terrorists plotting a missile attack during the opening Olympic ceremonies on February 8, 2002. The e-mails supposedly detailed plans to attack Salt Lake City with missiles launched from northern Russia.
He later confessed to making up the story during questioning, telling agents that stress led him to tell his tale and that he had fabricated the e-mails.

Just a few months ago, Federal prosecutors charged a University of Texas student with breaking into a school database and stealing more than 55,000 student, faculty and staff names and Social Security numbers in one of the nation's biggest cases of data theft involving a university. The student, a twenty-year old junior studying natural sciences, turned himself in at the U.S. Secret Service office in Austin, Texas. He was charged with unauthorized access to a protected computer and using false identification with intent to commit a federal offense. This incident sent a wave of fear across the campus of the nation's largest university, causing students and staff to consider replacing credit cards and freezing bank accounts. The student-perpetrator was released without bail and thereafter had limited access to computers. If convicted, the student faced as many as five years in prison and a $500,000 fine. After searching this student's Austin and Houston residences, Secret Service agents recovered the names and Social Security numbers on a computer in his Austin home. According to the indictment, Phillips wrote and executed a computer program in early March that enabled him to break into the university database that tracks staff attendance at training programs, reminding us how vulnerable we all are even when our Social Security number is misused. To combat the vulnerability linked to Social Security numbers, the university to limit its dependence on Social Security numbers as database identifiers and instead use an electronic identification number that matches only to Social Security numbers in an encrypted database. This data theft was probably the largest ever at a university.

Therefore, since the threat to critical infrastructure is realized at a very local level, we must channel our resources and technology to the first-responders and leaders in the local communities. The movement to securing our homeland needs to be expansive, not retractive. If our local hubs and first-responders are disabled by a terror threat, we would have a hard time developing effective protective measures for our nation as a whole.

Mr. Chairman, again, I thank you for your time and effort in this matter.

PREPARED STATEMENT OF THE HONORABLE BOB ETHERIDGE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Thank you, Chairman Thornberry and Ranking Member Lofgren, for holding this hearing. I would also like to welcome our witnesses to this important hearing on cybersecurity. I am looking forward to hearing how industry and academia view this issue.

Cybersecurity is a critical, yet elusive, concept for many people to grasp. You cannot see cyberterrorists attacking a network. There are no burning buildings or collapsing structures. When a virus hits our computers we may experience the annoyance of slow e-mail, spam or the inability to access the Internet. What we do not see until later are the costs in lost productivity and lost business in our electronically connected world. Since the Y2K bugs were worked out at the change of the millennium, cybersecurity has largely disappeared from the public consciousness. Yet, it is critical that the Department of Homeland Security encourage and foster research into protecting our country from these stealth attacks.

The Department must work in concert with private industry which not only owns more than 80 percent of our critical cyber infrastructure but also develops software products to run our businesses, our 911 emergency systems and our personal computers.

All of the witnesses today have made a number of suggestions for improving our nation's critical cyber infrastructure, and I am encouraged that they assign a great deal of responsibility to businesses to police their own systems and cooperate with the federal government in reporting attacks and breaches so that others may learn from the experience.

The Department of Homeland Security must promote science and math education for our children who will be our future software programmers and cyberwarriors. In the 2001 Hart-Rudman report "Road Map for National Security: Imperative for Change," the authors state that the greatest threat to our country, second only to the detonation of a weapon of mass destruction, would be "a failure to manage properly science, technology and education for the common good over the next quarter century."

A number of studies have shown that American students sorely lag behind their counterparts in other nations in science and math education. Even though they use computers every day for homework or to play games, many students who do go on to college do not enter technology fields because they see it as "too hard."

The federal government and private industry must work together with schools across the country to improve basic science and math education by providing teachers with the opportunities for advanced training in these fields, the proper equipment for labs and experiments, and time to teach. Gifted teachers prove every day that students can learn and come to love science and math. Our children are our future, and investment now in their education will provide benefits for many years to come.

Mr. THORNBERRY. I thank you, and I do want to thank the witnesses, too. We have had some scheduling back and forth for this hearing because of the full committee schedule, and I thank each of you for your flexibility and help in putting this on.

Finally I also want to thank Eric Fischer and his team at the Congressional Research Service who continue to help us in preparing for these hearings, as well as the folks in my office and Ms. Lofgren's office as well. Let me now turn to our witnesses. First we have Mr. Bruce Schneier, Founder and Chief Technical Officer of Counterpane Internet Security, Inc., a consulting firm specializing in cryptography and computer security. Mr. Schneier has written several books and articles. We are pleased to have you with us

today, and your full statement will be made part of the record and you may summarize it as you see fit.

STATEMENT OF BRUCE SCHNEIER, FOUNDER AND CHIEF TECHNICAL OFFICER, COUNTERPANE INTERNET SECURITY, INC.

Mr. SCHNEIER. Thanks for having me. I am actually the Founder and CTO of Counterpane, but I am not here under the auspices of Counterpane. I am probably going to say things counter to my company's interest, but I am here as a security expert, as an author, as a lecturer. So I do want to make that clear.

I was asked to talk about risks, and I talk about this in my written testimony. To summarize it very quickly, attacks are getting worse. I mean, every year we are seeing worse and worse attacks, primarily because, you know, hackers are getting more clever, and the tools they are writing are more interesting. At the same time, the expertise required to launch attacks is going down. Point/click interfaces—just as the word processors are easier to use, your hacker tools are easier to use.

There is a rise in crime, and I think this is a very important trend. We are seeing far more criminal activity on the Net. My company does a lot of security monitoring, and a lot of times the hardest problem we have is finding the criminal attacks amongst all the kids, amongst all the vandalism, amongst all the petty things.

Security is getting worse, and this is a hard thing to understand. I have written about it, and I urge you to read it. The complexity of software, of systems, causes lots of vulnerabilities, and these are getting worse faster than we are improving. Security products tend not to be very good. Software quality is abysmal. And I read the other testimonies you are going to hear, and we are all saying these sorts of things. The effect of this is that we are more and more insecure than we have ever been.

You said that we are also relying on the Internet more. So we are seeing more insecurities, yet it is more important; and this is a problem that I actually can't solve. This is not a technology problem, and what I really want to say in sort of my few minutes is how I need your help. This is a political problem, not a technology problem. The problem is that each company, each individual, installs security products, does security commensurate with their own risk. So a home user doesn't have much risk, doesn't care much, won't do much. A business will do whatever it has to do for its own risk. A software company will produce as secure a software as it has to.

The problem is most of the risks we face as a Nation are residual. So a company might have a risk to their business, but there is ancillary risk borne by everybody else, and that company is not going to secure itself to the level of the ancillary risk, only to the level of their risk. In economics it is called an externality. It is the effect of a decision that is not taken into account in the decision.

So an example might be—in environmentalism, a plant might pollute a river because it makes business sense, but the people living downstream don't factor into their decision. Someone might choose not to get married—a welfare mother might choose not to

get married because they will lose their welfare benefits, so they are making a rational decision based on their own interests; yet the effects to society of unwed people living together en masse, it doesn't factor in.

And computer security is largely stuck with these externalities, and that is the basic problem I have. And the way we deal with this in society is we try to somehow take those externalities and bring them into the decision. So laws and regulations are ways to do that. Liability is a way to do that. These are ways to make the effects of the actions of an individual organization, to make them responsible for them.

So for recommendations, I would like very much to see cybersecurity risks be subject to liabilities. To me it is absolutely insane that Firestone can produce a tire with a systemic flaw and be liable and for companies to produce software with, you know, three systemic flaws per month and not be liable. That just doesn't work. Liabilities will instantaneously improve security, because it will make it in a company's best interest to improve security.

I would like to see the government use its own purchasing power to improve security. You guys have enormous procurement power. I would like you to secure your own networks, secure your own systems, buy products and demand security. The nice thing about software is you do the work once, and everybody benefits. If you do massive procurement and design—give us secure systems, everybody will benefit.

This is not easy, all right? You are going to have other hearings. Software companies will tell you that liabilities will hurt them. Well, of course it will. An auto manufacturer will tell you the same thing. We would rather not be liable. We would like to produce features on our cars and we don't care if they crash.

I would like to see ISPs produce firewalls for their individuals. They will tell you that will hurt our business. Of course it will. Just like a building will tell you to making our building to fire codes makes it more expensive. Well, yes, it does. The point of security is that it costs money, and unless we make it so that it is in business's best interest to spend it, they won't. We can solve the technical problems if the business impetus is there. We can't do it without. And I am pleased to take questions after the other two gentlemen.

Mr. THORNBERRY. Thank you very much. I appreciate your testimony.

[The statement of Mr. Schneier follows:]

PREPARED STATEMENT MR. BRUCE SCHNEIER, FOUNDER AND CHIEF TECHNICAL OFFICER COUNTERPANE INTERNET SECURITY, INC.

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today regarding cybersecurity, particularly in its relation to homeland defense and our nation's critical infrastructure. My name is Bruce Schneier, and I have worked in the field of computer security for my entire career. I am the author of seven books on the topic, including the best-selling *Secrets and Lies: Digital Security in a Networked World* [1]. My newest book is entitled *Beyond Fear: Thinking Sensibly About Security in an Uncertain World [2],* and will be published in September. In 1999, I founded Counterpane Internet Security, Inc., where I hold the position of Chief Technical Officer. Counterpane Internet Security provides real-time security monitoring for hundreds of organizations, including several offices of the federal government.

Cyber Risks

When I began my long career in computer security, it was a marginal discipline. The only interest was from the military and a few scattered privacy advocates. The Internet has changed all that. The promise of the Internet is to be a mirror of society. Everything we do in the real world—all of our social and business interactions and transactions—we want to do on the Internet: conduct private conversations, keep personal papers, sign letters and contracts, speak anonymously, rely on the integrity of information, gamble, vote, publish authenticated documents. All of these things require security. Computer security is a fundamental enabling technology of the Internet; it's what transforms the Internet from an academic curiosity into a serious business tool. The limits of security are the limits of the Internet. And no business or person is without these security needs.

The risks are real. Everyone talks about the direct risks: theft of trade secrets, customer information, money. People also talk about the productivity losses due to computer security problems. What's the loss to a company if its e-mail goes down for two days? Or if ten people have to scramble to clean up after a particularly nasty intrusion? I've seen figures in the billions quoted for total losses from Internet epidemics like Nimda and the SQL Slammer; most of that is due to these productivity losses.

More important are the indirect risks: loss of customers, damage to brand, loss of goodwill. When a successful attack against a corporation is made public, the victim may experience a drop in stock price. When CD Universe suffered a large (and public) theft of credit card numbers in early 2000, it cost them dearly in their war for market share against Amazon.com and CDNow. In the aftermath of public corporate attacks, companies often spent more money and effort containing the public relations problem than fixing the security problem. Financial institutions regularly keep successful attacks secret, so as not to worry their customer base.

And more indirect risks are coming as a result of litigation. European countries have strict privacy laws; companies can be held liable if they do not take steps to protect the privacy of their customers. The U.S. has similar laws in particular industries—banking and healthcare—and there are bills in Congress to protect privacy more generally. We have not yet seen shareholder lawsuits against companies that failed to adequately secure their networks and suffered the consequences, but they're coming. Can company officers be held personally liable if they fail to provide for network security? The courts will be deciding this question in the next few years.

This hearing was convened to address another type of risk: the risks of our nation's critical infrastructure that is largely in the hands of private companies. One of the great challenges of cybersecurity is the interdependencies between individual networks. The security decisions one company makes about their own network can have far-reaching effects across many networks, and this leads us to different sorts of risks. I call these ancillary risks because their effects are ancillary to the particular network in question. Ancillary risks abound in cyberspace. For example, home computer users are at risk of attack and of having their machines taken over by others, but an ancillary risk is created when their attacked and taken-over computers can be used for further attacks against other networks. Vulnerabilities in software create a risk for the corporation marketing that software, but they also creates an ancillary risk for those who use that software in their networks.

The cybersecurity risks to our nation are largely ancillary; because our critical infrastructure is largely in the hands of private companies, there are risks to our nation that go beyond what those private companies are worried about. The telephone network has value to the telephone companies because that's how they get revenue, and those companies will secure their networks to that value. But the network has value to the country as a nationwide communications structure in addition to that, and there are ancillary risks as a result of that. Companies put themselves at risk when they purchase and use insecure software, but they also cause ancillary risks to everyone else on the Internet because that software is on a common network. These ancillary risks turn out to be critical to the current insecurities of cyberspace, and addressing them will give us the only real way to improve the situation.

As risky as the Internet is, companies have no choice but to be there. The lures of new markets, new customers, new revenue sources, and new business models are just so great that companies have flocked to the Internet regardless of the risks. There is no alternative. Governments feel the same sorts of pressures: better ways of interacting with citizens, more efficient ways of disseminating information, greater involvement of citizens in government. The Internet is here to stay, and we're going to be using it for more and more things regardless of the risks. This, more than anything else, is why computer security is so important.

Quantifying the Risks

Quantifying the risks is difficult, because we simply don't have the data. Most of what we know is anecdotal, and what statistics we have are difficult to generalize. In summary, cyberattacks are very common on the Internet. Corporations are broken into regularly, usually by hackers who have no motivation other than simple bragging rights. There is considerable petty vandalism on the Internet, and sometimes that vandalism becomes large-scale and system-wide. Crime is rising on the Internet, both individual fraud and corporate crime. We know all this is happening, because all surveys, corporate studies, and anecdotal evidence agree. We just don't know exact numbers.

For the past eight years, the Computer Security Institute has conducted an annual computer crime survey of U.S. corporations, government agencies, and other organizations [3]. The details are a bit numbing, but the general trends are that most networks are repeatedly and successfully attacked in a variety of ways, the monetary losses are considerable, and there's not much that technology can do to prevent it. In particular, the 2003 survey found the following:

- 56% of respondents reported "unauthorized use of computer systems" in the last year. 29% said that they had no such unauthorized uses, and 15% said that they didn't know. The number of incidents was all over the map, and the number of insider versus outsider incidents was roughly equal. 78% of respondents reported their Internet connection as a frequent point of attack (this has been steadily rising over the six years), 18% reported remote dial-in as a frequent point of attack (this has been declining), and 30% reported internal systems as a frequent point of attack (also declining).
- The types of attack range from telecommunications fraud to laptop theft to sabotage. 36% experienced a system penetration, 42% a denial-of-service attack. 21% reported theft of proprietary information, and 15% financial fraud. 21% reported sabotage. 25% had their Web sites hacked (another 22% didn't know), and 23% had their Web sites hacked ten or more times (36% of the Web site hacks resulted in vandalism, 35% in denial of service, and 6% included theft of transaction information).
- One interesting thing highlighted by this survey is that all of these attacks occurred despite the widespread deployment of security technologies: 98% have firewalls, 73% an intrusion detection system, 92% access control of some sort, 49% digital IDs. It seems that these much-touted security products provide only partial security against attackers.

Unfortunately, the CSI data is based on voluntary responses to surveys. The data only includes information about attacks that the companies knew about, and only those attacks that they are willing to admit to in a survey. Undoubtedly, the real numbers of attacks are much higher. And the people who complete the CSI survey are those experienced in security; companies who are much less security savvy are not included in this survey. These companies undoubtedly experience even more successful attacks and even higher losses.

The Honeynet Project is another source of data. This is an academic research project that measures actual computer attacks on the Internet. According to their most recent statistics [4], published in 2001, a random computer on the Internet is scanned dozens of times a day. The average life expectancy of a default installation of a Linux Red Hat 6.2 server—that is, the time before someone successfully hacks it—is less than 72 hours. A common home user setup, with Windows 98 and file sharing enabled, was successfully hacked five times in four days. Systems are subjected to hostile vulnerability scans dozens of times a day. And the fastest time for a server being hacked: 15 minutes after plugging it into the network. This data correlates with my own anecdotal experience of putting computers on an unsecured home broadband network.

At Counterpane Internet Security, we keep our own statistics. In 2002, we monitored several hundred computer networks in over thirty countries. We processed 160 billion network events, in which we uncovered 105 million security alerts. Further processing yielded 237,000 "tickets" which were investigated by our trained security analysts, resulting in 19,000 customer contacts from immediate security incidents. Assuming our data is representative, a typical company in the United States experiences 800 critical network security events—events requiring immediate attention—each year. At Counterpane we're smart and experienced enough to ensure that none of those events results in financial losses for the companies we protect, but most companies do not have such vigilant cyber guards.

Cybersecurity Trends

Several cybersecurity trends are worth highlighting. First, over the past few decades attacks on individual computers, early networks, and then the Internet have continually gotten more severe. Attack tools have gotten more potent, more damaging, more effective. Attacks that were once slow to implement are now automated. Attacks that used to be defeatable by a single mechanism are now adaptive. Viruses, worms, and Trojans are more elaborate and intelligent; malicious programs that years ago took weeks to spread across cyberspace, and last year took hours, today spread in minutes.

Second, over that same time period, the expertise required to launch those attacks has gone down. Many attack tools are easy to use. They have point-and-click interfaces. They are automated. They don't require any expertise to operate. "Root kits" are both easier to use and more effective.

These two trends combine to exacerbate another trend: the rise of crime in cyberspace. The vast majority of cyberspace attacks are nothing more than petty vandalism: the Internet equivalent of spray painting. The attackers aren't after anything except a cheap thrill and bragging rights. Sometimes they're bored teenagers. Sometimes they're smart kids with no other outlet. But we're starting to see significant increases in real crime on the Internet. Criminals, who often don't have the computer expertise to break into networks, can employ these easy-to-use tools to commit crimes. Credit card thefts and other forms of fraud are on the rise. Identity theft is on the rise. Extortion is on the rise. At Counterpane, often the hardest job we have is detecting these criminal attacks among the hundreds of petty vandalism attacks. I expect this trend to continue as more criminals discover the value of committing their frauds in cyberspace.

On the defensive side of things, cyberspace is becoming less secure even as security technologies improve. There are many reasons for this seemingly paradoxical phenomenon, but they can all be traced back to the problem of complexity. As I have said elsewhere [5], complexity is the worst enemy of security. The reasons are complex and can get very technical, but I can give you a flavor of the rationale: Complex systems have more lines of code and therefore more security bugs. Complex systems have more interactions and therefore more potential for insecurities. Complex systems are harder to test and therefore are more likely to have untested portions. Complex systems are harder to design securely, implement securely, configure securely, and use securely. Complex systems are harder for users to understand. Everything about complexity leads towards lower security. As our computers and networks become more complex, they inherently become less secure.

Another trend is the ineffectiveness of security products. This is not due to failures in technology, but more to failures of configuration and use. As amazing as it seems, the vast majority of security products are simply not implemented in ways that are effective. The blame could be laid on the products themselves, which are too hard to use. The blame could be laid on the system administrators, who often install security products without thinking too much about them. But the real blame is in the culture: security simply isn't a priority in most organizations. Security is routinely ignored, bypassed, or paid lip service to. Products are purchased because an organization wants to pass an audit or avoid litigation, but much less attention is paid to how they are used. It's as if a homeowner bought an expensive door lock and installed it in a way that didn't provide any security.

Along similar lines, the quality of software security is abysmal. Products routinely ship with hundreds or thousands of security vulnerabilities. Again, there are technical reasons for this. As a science, computer security is still in its infancy. We don't know, for example, how to write secure software. We have some tricks, and we know how to avoid some obvious problems, but we have no scientific theory of security. It's still a black art and, although we're learning all the time, we have a long way to go. But again, the real reason is that security isn't a priority for software vendors. It's far better for a company if they ship an insecure product a year earlier than a more secure product a year later.

The result of these trends is that security technologies are improving slowly, not nearly fast enough to keep up with the new insecurities brought about by the increasing complexity of systems. Every year brings more new attacks, faster-spreading worms, and more damaging malicious code. Software products—operating systems as well as applications software—continue to have more and more vulnerabilities. As long as the trends of increasing complexity and security's low priority continue, cyberspace will continue to become less secure.

Complexity is something we can't change. The only thing we can change is to make security a higher priority.

Cyberterrorism or "Digital Pearl Harbor"

There is one often-discussed trend that I do not see: the rise of cyberterrorism [6]. An essay I wrote on this issue is included as Attachment #1. I believe that fears about cyberterrorism, or the likelihood of a "Digital Pearl Harbor," are largely the result of companies and organizations wanting to stoke the fears of people and of the news media looking for sensationalist stories. Real terrorism—attacking the physical world via the Internet—is much harder than most people think, and the effects of cyber attacks are far less terrorizing than might seem at first. Cyberterrorism is simply not a problem that we have to worry about.

This does not mean that large-scale cyberspace threats are not a problem. A single vulnerability in a widely used software product can affect millions, and an attack that exploits that vulnerability can do millions of dollars of damage overnight. Attacks against popular Internet services, or critical information services that use the Internet to move data around, can affect millions.

While people overplay the risks of cyberterrorism, they underplay the risks of cyber-crime. Today credit card numbers are no longer being stolen one at a time out of purses and wallets; they're being stolen by the millions out of databases. Internet fraud is big business, and it's getting bigger.

And someday, cyberterrorism will become a real threat. Technology, especially technology related to cyberspace, is fast-moving and its effects are far-reaching. Just as some unknown attacker used the physical mail system to spread the anthrax virus, it is certainly possible that, someday, a terrorist may figure out how to kill large numbers of people via the Internet. But that day is not coming soon, and even then the same terrorist would probably have a much easier time killing the same number of people in a physical attack.

The Resilience of the Internet

Despite all of these risks, the Internet is reasonably safe from a catastrophic collapse. As insecure as each individual component or network that makes up the Internet is, as a whole it is surprisingly resilient. Often I have joked that the Internet "just barely works," that it is constantly being revised and upgraded, and that it's a minor miracle that it functions at all.

The Internet has seen examples of what many people have in mind when they think about large-scale attacks or terrorism, only they've been the result of accidents rather than maliciousness. Telephone switching stations shut down as the result of a software bug, leaving millions without telephone service. Communications satellites temporarily malfunctioned, disabling a nationwide pager network. On 9/11, the World Trade Center fell on much of lower Manhattan's communications network. What we've learned from these episodes is that the effects are not devastating and they're only temporary; communications can be quickly restored, and people adapt until they are restored.

Additionally, random events are still much more damaging than malicious actions. In the closest example of a cyberterrorist attack we've experienced, Vitek Boden hacked into a computer network and released a million liters of pollution into an Australian estuary. His damage was cleaned up in a week. A couple of months later, a bird landed on a transformer in the Ohio River valley, causing it to blow up; this set off a chain reaction that released about ten times as much sewage into the river. The cleanup was much more expensive and took significantly longer. Even today, random birds can do significantly more damage than the concerted effort of someone intent on damage.

Security and Risk Management

Companies manage risks. They manage all sorts of risks; cyber risks are just one more. And there are many different ways to manage risks. A company might choose to mitigate the risk with technology or with procedures. A company might choose to insure itself against the risk, or to accept the risk itself. The methods a company chooses in a particular situation depend on the details of that situation. And failures happen regularly; many companies manage their risks improperly, pay for their mistakes, and then soldier on. Companies, too, are remarkably resilient.

To take a concrete example, consider a physical store and the risk of shoplifting. Most grocery stores accept the risk as a cost of doing business. Clothing stores might put tags on their garments and sensors at the doorways; they mitigate the risk with technology. A jewelry store might mitigate the risk through procedures: all merchandise stays locked up, customers are not allowed to handle anything unattended, etc. And that same jewelry store will carry theft insurance, another risk management tool.

An appreciation of risk management is fundamental to understanding how businesses approach computer security. Ask any network administrator what he needs cybersecurity for, and he can describe the threats: Web site defacements, corruption

and loss of data due to network penetrations, denial-of-service attacks, viruses, and Trojans. The list of threats seems endless, and they're all real. Ask senior management about cybersecurity, and you'll get a very different answer. He'll talk about return on investment. He'll talk about risks. And while the cyber threats are great, the risks are much less so. What businesses need is adequate security at a reasonable cost.

Given the current state of affairs, businesses probably spend about the right amount on security. The threats are real and the attacks are frequent, but most of the time they're minor annoyances. Serious attacks are rare. Internet epidemics are rare. And on the other side of the coin, computer security products are often far less effective than advertised. Technology changes quickly, and it's hard to mitigate risks in such a rapidly changing environment. It is often more cost effective to weather the ill effects of bad security than to spend significant money trying to improve the level of security.

Externalities and Our Critical Infrastructure

If companies are so good at risk management, why not just let them manage their own risks? Companies can decide whether or not to have a guard in their corporate offices, install an alarm system in their warehouses, or buy kidnapping insurance for their key executives. Shouldn't we simply let companies make their own security decisions based on their own security risks? If they don't care whether they buy and use insecure software, if they don't bother installing security products correctly, if they don't implement good cybersecurity policies, why is that anyone else's problem? If they decide that it's cheaper to weather all the Internet attacks than it is to improve their own security, isn't it their own business?

The flaw in that argument is the reason this hearing was convened: the ancillary threats facing our nation's critical infrastructure. The risks to that infrastructure are greater than the sum of the risks to the individual companies. We need to protect ourselves against attack from an enemy military. We need to protect ourselves against a future where cyberterrorists may target our electronic infrastructure. We need to protect the underlying economic confidence in the Internet as a mechanism for commerce. We need to protect the Internet above the risks to individual pieces of it. Companies are good at risk management, but they're only going to consider their own risks; the ancillary risks to our critical infrastructure will not be taken into account.

One easy example is credit card numbers. Company databases are regularly broken into and credit card numbers are stolen, sometimes hundreds of thousands at a time. Companies work to secure those databases, but not very hard, because most of the risk isn't shouldered by those companies. When an individual finds that his credit card number has been stolen and used fraudulently or, even worse, that his entire identity has been stolen and used fraudulently, cleaning up the mess can take considerable time and money. The company secures the database based on its own internal risk; it does not secure the database based on the aggregate risk of all the individuals whose information it stores.

Software security is another example. Software vendors do some security testing on their products, but it's minimal because most of the risk isn't their problem. When a vulnerability is discovered in a software product, the vendor fixes the problem and issues a patch. This costs some money, and there's some bad publicity. The real risk is shouldered by the companies and individuals who purchased and used the product, and that risk doesn't affect the vendor nearly as much. When the SQL Slammer worm spread across the Internet in January 2003, worldwide losses were calculated in the tens of billions of dollars. But the losses to Microsoft, whose software contained the vulnerability that the Slammer used in the first place, were much, much less. Because most of the risks to Microsoft are ancillary, security isn't nearly as high a priority for them as it should be.

This brings us to the fundamental problem of cybersecurity: It needs to be improved, but those who can improve it—the companies that build computer hardware and write computer software, and the people and companies that own and administer the small networks that make up the Internet—are not motivated to do so.

More specifically: Our computers and networks are insecure, and there every reason to believe that they will become less secure in the future. The threats and risks are significant, and there is every reason to believe that they will become more significant in the future. But at the same time, because much of the risks are ancillary, software and hardware manufacturers don't spend a lot of money improving the security of their products and private network owners don't spend a lot of money buying and installing security products on their networks.

In economics, an externality is an effect of a decision that is not part of the decision process. Most pollution, for example, is an externality. A factory makes an eco-

nomic decision about the amount of pollution it dumps into a river based on its own economic motivations; the health of the people living downstream is an externality. A welfare mother makes a decision whether to marry someone or live with him without marriage partly based on the economics of the welfare system; the societal degradation of the institution of marriage is an externality. Ancillary cyberrisks are an example of an externality.

There are several ways to deal with externalities. They can be regulated through a legal system: Laws and regulations which prohibit certain actions and mandate others are a way to manage externalities. They can be internalized through taxation or liabilities, both of which provide economic incentives to take externalities into account. Sometimes societal norms modify externalities. And so on. The particular mechanism chosen will depend on politics, but the overall goal is to bring the various externalities into the decision process.

I believe that externalities are the fundamental problem of cybersecurity. The security of a particular piece of the Internet may be good enough for the organization controlling that piece, but the external effects of that "good enough" security may not be good enough for the nation as a whole. Our nation's critical infrastructure is becoming more and more dependent on a secure and functioning Internet, but there's no one organization in charge of keeping the Internet secure and functioning. Our software has very poor security, and there is no real incentive to make it better. We are increasingly vulnerable to attacks that affect everyone a little bit, but that no one has enough incentive to fix.

Recommendations

This fundamental problem of cybersecurity is much more an economic one than a technical one. Our nation's computer infrastructure could be much more secure if the business incentives were there to make it so—if the externalities were internalized, so to speak. Asking companies to improve their own security won't work. (We've tried this repeatedly; it's doomed to failure.) Trying to build a separate government network won't work. (The whole point of cyberspace is that it is one large interconnected network.) Hoping technology will improve won't work. (It doesn't matter how good the technology is if people don't want to use it.)

The basic capitalist and democratic business process is capable of improving cybersecurity, but only if the proper incentives are in place. My general recommendation is that you pass laws and implement regulations designed to deal with the externalities in cybersecurity decisions so that organizations are motivated to provide a higher level of security—one that is commensurate with the threat against our nation's critical infrastructure—and then step back and let the mechanisms of commercial innovation work to solve the problems and improve security. Specifically:

1. Stop trying to find consensus. Over the years, we have seen several government cyberspace security plans and strategies come out of the White House, the most recent one this year [7]. These documents all suffer from an inability to risk offending any industry. In the most recent strategy, for example, preliminary drafts included strong words about wireless insecurity that were removed at the request of the wireless industry, which didn't want to look bad for not doing anything about it. A recommendation that ISPs provide personal firewalls to all of their users was likewise removed, because the large ISPs didn't want to look bad for not already providing such a security feature. Unlike many other governmental processes, security is harmed by consensus. Cybersecurity requires hard choices. These choices will necessarily come at the expense of some industries and some special interests. As long as the government is unwilling to move counter to the interests of some of its corporate constituents, huge insecurities will remain.

2. Expose computer hardware, software, and networks to liabilities. I have written extensively about the effect of liabilities on the computer industry [8]; one of my essays is included as Attachment #2. The major reason companies don't worry about the externalities of their security decisions—the effects of their insecure products and networks on others—is that there is no real liability for their actions. Liability will immediately change the cost/benefit equation for companies, because they will have to bear financial responsibility for ancillary risks borne by others as a result of their actions. With liabilities firmly in place, the best interests of software vendors, and the best interests of their shareholders, will be served by them spending the time and money necessary to make their products secure before release. The best interests of corporations, and the best interests of their shareholders, will be served by them spending the time and money necessary to secure their own networks. The insurance industry will step in and force companies to improve their own security if they want liability coverage at a reasonable price. Liability is a com-

mon capitalistic mechanism to deal with externalities, and it will do more to secure our nation's critical infrastructure than any other action.

3. Secure your own networks. Fund programs to secure government networks, both internal networks and publicly accessible networks. Only buy secure hardware and software products. Before worrying about the security of everyone else, get your own house in order. This does not mean that it's necessary to redo what is already being done in industry. The government is a consumer of computer products, like any large corporation. The government does not need to develop its own security products; everyone's security is better served if the government buys commercial products. The government does not need to create its own organization to identify and analyze cyber threats; it is better off using the same commercial organizations that corporations use. The threats against government are the same as the threats against everyone else, and the solutions are the same. The U.S. government, specifically the Department of Homeland Security, should use and improve the resources that are available to everyone, since everyone needs those same resources.

4. Use your buying power to drive an increase in security. U.S. government procurement can be a potent tool to drive research and development. If you demand more secure products, companies will deliver. Standardize on a few good security products, and continually force them to improve. There's a "rising tide" effect that will happen; once companies deliver products to the increasingly demanding specifications of the government, the same products will be made available to private organizations as well. The U.S. government is an enormous consumer of computer hardware, software, systems, and services. And because you're using the same commercial products that everyone else uses, those products will improve to the benefit of everyone. The money you spend on your own security will benefit everyone's security.

5. Invest in security research; invest in security education. As the market starts demanding real security, companies will need to figure out how to supply it. Research and education are critical to improving the security of computers and networks. Here again, use your financial muscle to improve security for everyone. Research and education in this important field need to be increased. The benefits will be beyond anything we can imagine today.

6. Rationally prosecute cybercriminals. In our society, we rarely solve security problems by technical means alone. We don't wear body armor or live in fortresses. Instead, we rely on the legal system to rationally prosecute criminals and act as a deterrent to future crimes. We need to beef up law enforcement to deal with real computer crimes. This does not mean charging sixteen-year-old kids as adults for what are basically 21st century pranks; this means going after those who commit real crimes on the Internet.

Conclusion

None of this is easy. Every computer company you bring into this room will tell you that liabilities will be bad for their industry. Of course they're going to tell you that; it's in their best interests not to be responsible for their own actions. The Department of Homeland Security will tell you that they need money for this and that massive government security program. Of course they're going to tell you that; it's in their best interests to get as large a budget as they can. The FBI is going to tell you that extreme penalties are necessary for the current crop of teenage cyberterrorists; they're trying to make the problem seem more dire than it really is to improve their own image. If you're going to help improve the security of our nation, you're going to have to look past everyone's individual self-interests toward the best interests of everyone.

Our nation's cybersecurity risks are greater than those of any individual corporation or government organization, and the only way to manage those risks is to address them directly. I strongly recommend that you put the interests of our nation's cybersecurity above the interests of individual corporations or government organizations. The externalities of rational corporate cybersecurity decisions are hurting us all. It's the job of government to look at the big picture and the needs of society as a whole, and then to properly motivate individuals to satisfy those needs.

Thank you for the opportunity to appear before your committee today. I would be pleased to answer any questions.

References

[1] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World,* John Wiley & Sons, 2000.
[2] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World,* Copernicus Books, 2003.
[3] Computer Security Institute, "2003 CSI/FBI Computer Crime and Security Survey," 2003. http://www.gocsi.com/press/20030528.html
[4] Honeynet Project, :Know Your Enemy: Statistics," 22 July, 2001. http://www.honeynet.org/papers/stats/
[5] Bruce Schneier, "Software Complexity and Security," *Crypto-Gram,* March 15, 2000. http://www.counterpane.com./crypto-gram-0003.html
[6] Bruce Schneier, "The Risks of Cyberterrorism," *Crypto-Gram,* June 15, 2003. http://www.counterpane.com./crypto-gram-0306.html
[7] White House, *National Strategy to Secure Cyberspace,* Feb 2003. http://www.whitehouse.gov/pcipb/cyberspace—strategy.pdf
[8] Bruce Schneier, "Liability and Security," *Crypto-Gram,* April 15, 2002. http://www.counterpane.com./crypto-gram-0204.html

ATTACHMENT #1

The Risks of Cyberterrorism

Bruce Schneier

Reprinted from: *Crypto-Gram,* June 15, 2003.

http://www.counterpane.com./crypto-gram-0306.html

The threat of cyberterrorism is causing much alarm these days. We have been told to expect attacks since 9/11; that cyberterrorists would try to cripple our power system, disable air traffic control and emergency services, open dams, or disrupt banking and communications. But so far, nothing's happened. Even during the war in Iraq, which was supposed to increase the risk dramatically, nothing happened. The impending cyberwar was a big dud. Don't congratulate our vigilant security, though; the alarm was caused by a misunderstanding of both the attackers and the attacks. These attacks are very difficult to execute. The software systems controlling our nation's infrastructure are filled with vulnerabilities, but they're generally not the kinds of vulnerabilities that cause catastrophic disruptions. The systems are designed to limit the damage that occurs from errors and accidents. They have manual overrides. These systems have been proven to work; they've experienced disruptions caused by accident and natural disaster. We've been through blackouts, telephone switch failures, and disruptions of air traffic control computers. In 1999, a software bug knocked out a nationwide paging system for a day. The results might be annoying, and engineers might spend days or weeks scrambling, but the effect on the general population has been minimal.

The worry is that a terrorist would cause a problem more serious than a natural disaster, but this kind of thing is surprisingly hard to do. Worms and viruses have caused all sorts of network disruptions, but it happened by accident. In January 2003, the SQL Slammer worm disrupted 13,000 ATMs on the Bank of America's network. But before it happened, you couldn't have found a security expert who understood that those systems were dependent on that vulnerability. We simply don't understand the interactions well enough to predict which kinds of attacks could cause catastrophic results, and terrorist organizations don't have that sort of knowledge either—even if they tried to hire experts.

The closest example we have of this kind of thing comes from Australia in 2000. Vitek Boden broke into the computer network of a sewage treatment plant along Australia's Sunshine Coast. Over the course of two months, he leaked hundreds of thousands of gallons of putrid sludge into nearby rivers and parks. Among the results were black creek water, dead marine life, and a stench so unbearable that residents complained. This is the only known case of someone hacking a digital control system with the intent of causing environmental harm.

Despite our predilection for calling anything "terrorism," these attacks are not. We know what terrorism is. It's someone blowing himself up in a crowded restaurant, or flying an airplane into a skyscraper. It's not infecting computers with viruses, forcing air traffic controllers to route planes manually, or shutting down a pager network for a day. That causes annoyance and irritation, not terror.

This is a difficult message for some, because these days anyone who causes widespread damage is being given the label "terrorist." But imagine for a minute the leadership of al Qaeda sitting in a cave somewhere, plotting the next move in their jihad against the United States. One of the leaders jumps up and exclaims: "I have an idea! We'll disable their e-mail...." Conventional terrorism—driving a truckful of explosives into a nuclear power plant, for example—is still easier and much more effective.

There are lots of hackers in the world—kids, mostly—who like to play at politics and dress their own antics in the trappings of terrorism. They hack computers belonging to some other country (generally not government computers) and display a political message. We've often seen this kind of thing when two countries squabble: China vs. Taiwan, India vs. Pakistan, England vs. Ireland, U.S. vs. China (during the 2001 crisis over the U.S. spy plane that crashed in Chinese territory), the U.S. and Israel vs. various Arab countries. It's the equivalent of soccer hooligans taking out national frustrations on another country's fans at a game. It's base and despicable, and it causes real damage, but it's cyberhooliganism, not cyberterrorism.

There are several organizations that track attacks over the Internet. Over the last six months, less than 1% of all attacks originated from countries on the U.S. government's Cyber Terrorist Watch List, while 35% originated from inside the United States. Computer security is still important. People overplay the risks of cyberterrorism, but they underplay the risks of cybercrime. Fraud and espionage are serious problems. Luckily, the same countermeasures aimed at cyberterrorists will also prevent hackers and criminals. If organizations secure their computer networks for the wrong reasons, it will still be the right thing to do.

ATTACHMENT #2

Liability and Security

Bruce Schneier

Reprinted from: *Crypto-Gram,* April 15, 2002.http://www.counterpane.com./crypto-gram-0204.html

Today, computer security is at a crossroads. It's failing, regularly, and with increasingly serious results. I believe it will improve eventually. In the near term, the consequences of insecurity will get worse before they get better. And when they get better, the improvement will be slow and will be met with considerable resistance. The engine of this improvement will be liability—holding software manufacturers accountable for the security and, more generally, the quality of their products—and the timetable for improvement depends wholly on how quickly security liability permeates cyberspace.

Network security is not a problem that technology can solve. Security has a technological component, but businesses approach security as they do any other business risk: in terms of risk management. Organizations optimize their activities to minimize their cost * risk product, and understanding those motivations is key to understanding computer security today.

For example, most organizations don't spend a lot of money on network security. Why? Because the costs are significant: time, expense, reduced functionality, frustrated end users. On the other hand, the costs of ignoring security and getting hacked are small: the possibility of bad press and angry customers, maybe some network downtime, none of which is permanent. And there's some regulatory pressure, from audits or lawsuits, that add additional costs. The result: a smart organization does what everyone else does, and no more.

The same economic reasoning explains why software vendors don't spend a lot of effort securing their products. The costs of adding good security are significant—large expenses, reduced functionality, delayed product releases, annoyed users—while the costs of ignoring security are minor: occasional bad press, and maybe some users switching to competitors' products. Any smart software vendor will talk big about security, but do as little as possible.

Think about why firewalls succeeded in the marketplace. It's not because they're effective; most firewalls are installed so poorly as not to be effective, and there are many more effective security products that have never seen widespread deployment. Firewalls are ubiquitous because auditors started demanding firewalls. This changed the cost equation for businesses. The cost of adding a firewall was expense and user annoyance, but the cost of not having a firewall was failing an audit. And even worse, a company without a firewall could be accused of not following industry best practices in a lawsuit. The result: everyone has a firewall, whether it does any good or not.

Network security is a business problem, and the only way to fix it is to concentrate on the business motivations. We need to change the costs; security needs to affect an organization's bottom line in an obvious way. In order to improve computer security, the CEO must care. In order for the CEO to care, it must affect the stock price and the shareholders.

I have a three-step program towards improving computer and network security. None of the steps have anything to do with the technology; they all have to do with businesses, economics, and people.

Step one: enforce liabilities. This is essential. Today there are no real consequences for having bad security, or having low-quality software of any kind. In fact, the marketplace rewards low quality. More precisely, it rewards early releases

at the expense of almost all quality. If we expect CEOs to spend significant resources on security—especially the security of their customers—they must be liable for mishandling their customers' data. If we expect software vendors to reduce features, lengthen development cycles, and invest in secure software development processes, they must be liable for security vulnerabilities in their products.

Legislatures could impose liability on the computer industry, by forcing software manufacturers to live with the same product liability laws that affect other industries. If software manufacturers produced a defective product, they would be liable for damages. Even without this, courts could start imposing liability-like penalties on software manufacturers and users. This is starting to happen. A U.S. judge forced the Department of Interior to take its network offline, because it couldn't guarantee the safety of American Indian data it was entrusted with. Several cases have resulted in penalties against companies who used customer data in violation of their privacy promises, or who collected that data using misrepresentation or fraud. And judges have issued restraining orders against companies with insecure networks that are used as conduits for attacks against others.

However it happens, liability changes everything. Currently, there is no reason for a software company not to offer more features, more complexity. Liability forces software companies to think twice before changing something. Liability forces companies to protect the data they're entrusted with.

Step two: allow parties to transfer liabilities. This will happen automatically, because this is what insurance companies do. The insurance industry turns variable-cost risks into fixed expenses. They're going to move into cyber-insurance in a big way. And when they do, they're going to drive the computer security industry. . .just like they drive the security industry in the brick-and-mortar world.

A company doesn't buy security for its warehouse—strong locks, window bars, or an alarm system—because it makes it feel safe. It buys that security because its insurance rates go down. The same thing will hold true for computer security. Once enough policies are being written, insurance companies will start charging different premiums for different levels of security. Even without legislated liability, the CEO will start noticing how his insurance rates change. And once the CEO starts buying security products based on his insurance premiums, the insurance industry will wield enormous power in the marketplace. They will determine which security products are ubiquitous, and which are ignored. And since the insurance companies pay for the actual liability, they have a great incentive to be rational about risk analysis and the effectiveness of security products.

And software companies will take notice, and will increase security in order to make the insurance for their products affordable.

Step three: provide mechanisms to reduce risk. This will happen automatically, and be entirely market driven, because it's what the insurance industry wants. Moreover, they want it done in standard models that they can build policies around. They're going to look to security processes: processes of secure software development before systems are released, and processes of protection, detection, and response for corporate networks and systems. And more and more, they're going to look towards outsourced services.

The insurance industry prefers security outsourcing, because they can write policies around those services. It's much easier to design insurance around a standard set of security services delivered by an outside vendor than it is to customize a policy for each individual network.

Actually, this isn't a three-step program. It's a one-step program with two inevitable consequences. Enforce liability, and everything else will flow from it. It has to.

Much of Internet security is a common: an area used by a community as a whole. Like all commons, keeping it working benefits everyone, but any individual can benefit from exploiting it. (Think of the criminal justice system in the real world.) In our society we protect our commons—our environment, healthy working conditions, safe food and drug practices, lawful streets, sound accounting practices—by legislating those goods and by making companies liable for taking undue advantage of those commons. This kind of thinking is what gives us bridges that don't collapse, clean air and water, and sanitary restaurants. We don't live in a "buyer beware" society; we hold companies liable for taking advantage of buyers.

There's no reason to treat software any differently from other products. Today Firestone can produce a tire with a single systemic flaw and they're liable, but Microsoft can produce an operating system with multiple systemic flaws discovered per week and not be liable. This makes no sense, and it's the primary reason security is so bad today.

Mr. THORNBERRY. And before turning to the next witness, let me thank the distinguished chairman of the Science Committee for allowing us the use of your facilities. As we continue to be homeless, we appreciate the chairman's generosity.

Our next witness is Richard Pethia, Director of CERT Centers, Software Engineering Institute, Carnegie Mellon University. CERT provides the central response and coordination facility for global information security instant response and countermeasures for cyber threats and vulnerabilities since 1988. We appreciate you being with us, sir. Your full statement will also be made a part of the record, and please summarize it as you would like.

STATEMENT OF RICHARD D. PETHIA

Mr. PETHIA. First, thank you, Mr. Chairman, members of the subcommittee, for the opportunity to testify on cybersecurity issues. It is something that we in Pittsburgh have been working on for a number of years and feel very passionate about.

The current state of Internet security from our perspective is cause for concern. Security issues are not well understood. They are rarely given high priority by many software developers, vendors, network managers or consumers. At the same time, however, computers have become such an integral part of American government and business operation, that computer-related risk can no longer be separated from national defense, general safety, health, business and privacy risks.

We are increasingly dependent on our computers and the networks that hook them together, or planes won't fly, freight won't ship, oil won't pump, the things that—the physical things in our lives are as critically dependent on these systems are as things like financial transactions and business transactions that we all recognize.

The data that we have and data from other groups in the security field indicates that the attacks are going up year after year. The damage is increasing, and that is happening even while government and the industry are actually investing increasing amounts of money to deal with the problem.

There are a number of factors that contribute to this increased vulnerability. First of all, we are connecting everything to everything else. For many good business reasons, we are connecting more and more of our systems to the Internet. The phone system, the Internet, are merging and we are building a communications fabric where everything is tied together. And a number of systems, where once secure because of their isolation, are now insecure because they are connected to this web of computing that we have constructed.

Cyberspace and physical space are becoming one. Supervisory control and data acquisition systems that control power grids, water treatment and distribution plans, oil and chemical refineries, other physical processes, are being linked to communications links in the Internet, and these systems are becoming potential targets of individuals bent on causing massive disruption and physical damage.

Engineering for ease of use is driving a dramatic increase in the use of computers, but at the same time it is not been matched by

engineering for ease of secure administration. The result is increasing numbers of vulnerable computers. Comprehensive security solutions are lacking. Engineering the security of a large complex system is often more difficult than engineering the system itself, and many organizations just don't have the skills.

The Internet at the same time has become a virtual breeding ground for attackers. Intruders share information about vulnerable sites, about vulnerabilities in technology and attack tools. Internet attacks are difficult to trace, and the protocols make it easy for attackers to hide their true identity and location.

With all these factors, there are two others that I think are especially important to focus on. One is vulnerabilities in the information technology products in the market today.

Last year we received reports of over 4,000 separate new vulnerabilities. Weaknesses in products that an attacker can exploit compromise a system. Some of these are deep-seated and are likely to be long-lived, in that they are the result of architecture and design decisions that were made early in the product's development cycle, not decisions that can be changed easily.

Others are the result of weak implementation in testing practices, bugs in the program. They can be quickly corrected. However, both of these require that system operators take action to protect their systems, and with so many of these problems being found every year, it is placing the system operators in a very hard spot. They have got a major challenge.

The second major rea of vulnerability includes weakness in the management and operational practice of the system operators themselves. Typical problems include things like poor or ambiguous security policies, lack of security training for all levels of staff, poor account and access management, poor physical security, leading to open access to critical devices, lack of vulnerability management practices and lack of monitoring or auditing to detect security weaknesses and attacks.

Putting these practices in place requires senior management understanding and commitment, and that is a condition that is still missing in many organizations. Working our way out of this vulnerable position will require a multipronged approach. First, hire quality products. Good software engineering practices can dramatically improve our ability to withstand attacks. We need operating systems and other products that are virtually virus-proof. We need to reduce the implementation errors that we have by at least two orders of magnitude, and we need to have vendors ship products with high security default configurations.

We encourage the government to use its buying power to demand such high-quality software. Acquisition processes must be in place with more emphasis on security characteristics and perhaps the use of code integrity clauses that hold vendors more accountable for defects in their release products. Acquisition professionals should be trained in government security regulations and policies and also in the fundamentals of security concepts and architectures.

Also needed is wider adoption of security practices. Senior management must be accountable for the use of the technology in their operation, and they must provide visible endorsement of security

improvement efforts and the resources needed to implement those required improvements.

And in the long term, research has to be an essential component of the answer. We need a unified and integrated framework for all information assurance analysis that leads to a new generation of products that are fundamentally more secure than those we have today. We need more rigorous methods to assess and manage risks and quantitative techniques to help us understand the cost/benefit analysis of doing that risk mitigation, along with simulation tools to analyze the cascade effects of attacks, accidents, and failures across our interdependent systems.

We as a Nation need more qualified technical specialists. The government scholarship programs that are in place need to be expanded over the next 5 years to build an infrastructure that will meet the long-term needs of trained security professionals, and also needed is more awareness and security training for all Internet and technology users.

So in conclusion, the incidents are almost doubling every year, and the attack technology will evolve to support attacks that are even more virulent and damaging. We can make significant progress by making changes in our software design and development practices, giving more management support to risk management activities, increasing the number of trained system managers and administrators, and increasing research in the secure and survivable systems. Thank you.

Mr. THORNBERRY. Thank you. Appreciate it.

[The statement of Mr. Pethia follows:]

PREPARED STATEMENT OF RICHARD D. PETHIA

1. Introduction

Mr. Chairman and members of the Subcommittee: My name is Rich Pethia. I am the director of the CERT Centers, part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We have 14 years of experience with computer and network security. The CERT Coordination Center (CERT/CC) was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, acting as a wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled well over 200,000 incidents and cataloged more than 8,000 computer vulnerabilities.

Thank you for the opportunity to testify on cyber security problem. Today I will discuss the vulnerability of information technology on the Internet and steps I believe we must take to better protect our critical systems from future attacks.

The current state of Internet security is cause for concern. Vulnerabilities associated with the Internet put users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Security issues are often not well understood and are rarely given high priority by many software developers, vendors, network managers, or consumers.

Government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently many of the day-to-day operations depend upon connections to the Internet, and new connections are continuously being made to the Internet. Use of the Internet enhances the ability of organizations to conduct their activities in a cost-effective and efficient way. However, along with increased capability and dependence comes increased vulnerability. It is easy to exploit the many security holes in the Internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Moreover, the Internet is easily accessible to anyone with a

computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

Computers have become such an integral part of American business and government that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable government and business assets are now at risk over the Internet. For example, customer and personnel information may be exposed to intruders. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

Techniques that have worked in the past for securing isolated systems are not effective in the world of unbounded networks, mobile computing, distributed applications, and dynamic computing that we live in today. Today there is rapid movement toward increased use of interconnected networks for a broad range of activities, including commerce, education, entertainment, operation of government, and supporting the delivery of health and other human services. Although this trend promises many benefits, it also poses many risks. In short, interconnections are rapidly increasing and opportunities to exploit vulnerabilities in the interconnected systems are increasing as well.

2. Key Factors in the Current State of Internet Security

The current state of Internet security is the result of many factors. A change in any one of these can change the level of Internet security and survivability.

• We are connecting everything with everything else. Because of the dramatically lower cost of communication and ease of connecting to the Internet, use of the Internet is replacing other forms of electronic communication. As critical infrastructure operators strive to improve their efficiency and lower costs, they are connecting formerly isolated systems to the Internet to facilitate remote maintenance functions and improve coordination across distributed systems. Operations of the critical infrastructures are becoming increasingly dependent on the Internet and are vulnerable to Internet based attacks.

• Cyber space and physical space are becoming one. Most threatening of all is the link between cyber space and physical space. Supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have for years been used to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems. Increasingly, these control systems are being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions. These computer-controlled and network-connected systems are potential targets of individuals bent on causing massive disruption and physical damage. This is not just theory; actual attacks have caused major operational problems. Attacks against wastewater treatment systems in Australia, for example, led to the release of hundreds of thousands of gallons of sludge.

• There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, the management of the technology is often distributed as well. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely.

• The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess password increases an organization's risk.

• There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. In 1995 we received an average of 35 new reports each quarter, 140 for the year. By 2002, the number of annual reports received had skyrocketed to over 4000. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change.

• When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the need for system administrators with strong security skills far exceeds the supply.
• Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.
• As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.
• Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. Although some attacks seem playful (for example, students experimenting with the capability of the network) and some are clearly malicious, all have the potential of doing damage. Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker. While some attacks require technical knowledge—the equivalent to that of a college graduate who majored in computer science—many other successful attacks are carried out by technically unsophisticated intruders. Technically competent intruders duplicate and share their programs and information at little cost, thus enabling novice intruders to do the same damage as the experts. In addition to being easy and cheap, Internet attacks can be quick. In a matter of seconds, intruders can break into a system; hide evidence of the break-in; install their programs, leaving a "back door" so they can easily return to the now-compromised system; and begin launching attacks at other sites.
• Attackers can lie about their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination. Senders provide their return address, but they can lie about it. Most of the Internet is designed merely to forward packets one step closer to their destination with no attempt to make a record of their source. There is not even a "postmark" to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack. Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort. This means that it is easy for an adversary to use a foreign site to launch attacks at U.S. systems. The attacker enjoys the added safety of the need for international cooperation in order to trace the attack, compounded by impediments to legal investigations. We have seen U.S.-based attacks on U.S. sites gain this safety by first breaking into one or more non-U.S. sites before coming back to attack the desired target in the U.S.

3. Categories of vulnerabilities

Protecting any complex system (hardware, software, people, and physical plant) and insuring its successful operation in the face of attacks, accidents and failures is a difficult task. Vulnerabilities (weaknesses that can be exploited to compromise the operation of the system) can creep into the system in a variety of areas. Deciding which vulnerabilities really matter and effectively dealing with them, are key steps in an organization's risk management process.

For discussion, it is useful to separate sources of vulnerability into two major categories: weaknesses in the information technology (IT) products as supplied by the vendor(s); and weakness in the ways organizations manage and use the technology.

IT Product Vulnerabilities

As stated above, the number of vulnerabilities in IT products discovered each year is increasing dramatically: from 140 reported to the CERT/CC in 1995 to 4,129 reported in 2002. Each vulnerability represents a weakness in a product that can be exploited in some way to help an attacker achieve the objective of compromising a system.

Some of these vulnerabilities are deep-seated and difficult to correct because they are the result of architecture and design decisions that were made early in the product's development cycle (e.g. operating system architectures that allow the unconstrained execution of application software and thereby allow the easy propagation of viruses). In these cases, the vulnerabilities can only be removed by changing the basic architecture of the product. These types of fundamental changes often have consequences that affect other aspects of the product's operation. In some cases these side effects will cause applications that inter-operate with the product to "break" (i.e. the new version of the product is no longer compatible with earlier versions and users may need to rewrite their applications). These types of vulnerability are typically long-lived and product users must find some other way to protect themselves from attacks that attempt to exploit the vulnerability (e.g. invest in anti-virus software in order to detect and remove viruses before they operate on the vulnerable system).

Other vulnerabilities are easier to correct since they are the result of low-level design decisions or implementation errors (bugs in the programs). It is often that case that these types of vulnerability, once discovered, can quickly be corrected by the vendor and the corrections (oftentimes called "patches") made available to the customers. However, even though the corrections may be available quickly, it is not always the case that they can be deployed quickly. System operators need to insure that the corrections do not have unintended side-effects on their systems and typically test the corrections before deployment. Also, in the case of a widely used product, system operators must often update the software used in thousands of computers to deploy the correction. This in itself is a labor intensive and time consuming task.

In either case, IT product vulnerabilities are often long-lived with many Internet connected systems vulnerable to a particular form of attack many months after vendors produce corrections to the vulnerability that was exploited by the attack.

Weaknesses in Management and Operational Practice

The second major category of vulnerability includes weaknesses in the management and operational practices of system operators. Factors that lead to weaknesses in operational practices include things like:

- Lack of, ambiguous or poorly enforced organizational security policies and regulations; security roles and responsibilities that are not clearly defined or lack of accountability
- Failure to account for security when outsourcing IT services
- Lack of security awareness training for all levels of staff
- Poor account management or password management by all users
- Poor physical security leading to open access to important computers and network devices
- Weak configuration management practices that allow for vulnerable configurations
- Weak authentication practices that allow attackers to masquerade as valid system users
- Lack of vulnerability management practices that require system administrators to quickly correct important vulnerabilities
- Failure to use strong encryption when transmitting sensitive information over the network.
- Lack of monitoring and auditing practices that can detect attacker behavior before damage is done.

Weaknesses in any of these areas open the doors for attackers and give them opportunities to take advantage of the weaknesses to achieve their goals. Managing the risk associated with this category of vulnerability requires that organizations dedicate resources to the risk management task. Operations must be continuously assessed and corrective actions taken when needed.

4. Recommended Actions

Working our way out of the vulnerable position we are in requires a multi-pronged approach that helps us deal with the escalating near-term problem while at the same time building stronger foundations for the future. The work that must be done includes achieving these changes:

- Higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users

- Wider adoption of risk analysis and risk management policies and practices that help organizations identify their critical security needs, assess their operations and systems against those needs, and implement security improvements identified through the assessment process
- Expanded research programs that lead to fundamental advances in computer security
- A larger number of technical specialists who have the skills needed to secure large, complex systems
- Increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Higher quality products: In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- Virus-resistant/virus-proof software—There is nothing intrinsic about digital computers or software that makes them vulnerable to viruses, which propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow the unconstrained execution of that code on the machine that received it. Unconstrained execution allows code developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.
- Reducing implementation errors by at least two orders of magnitude—Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while in use. Worse, the same flaws continue to be introduced in new products. Vendors need to be proactive, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- High-security default configurations—With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" configurations if desired, but they would have the benefit of starting from a secure base.

To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses, clauses that hold vendors more accountable for defects in released products. Included here as well are upgraded acquisition processes that place more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, training programs for acquisition professionals should be developed that provide training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is needed in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.
Wider adoption of security practices: With our growing dependence on information networks and with the rapid changes in network technology and threats, it is critical that more organizations, large and small, adopt the use of effective information security risk assessments, management policies, and practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources such as the National Institute of Standards and Technology, the National Security Agency, and other agencies. What is often missing today is management commitment: senior management's visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

Expanded research in information assurance: It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield

networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

In this research program, special emphasis should be placed on the overlap between the cyber world and the physical world, and the analysis techniques developed should help policy and decision makers understand the physical impact and disruption of cyber attacks alone or of cyber attacks launched to amplify the impact of concurrent physical attacks.

More technical specialists: Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users: The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one's own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.[1] Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

5. Conclusion

Interconnections across and among cyber and physical systems are increasing. Our dependence on these interconnected systems is also rapidly increasing, and even short-term disruptions can have major consequences. Cyber attacks are cheap, easy to launch, difficult to trace, and hard to prosecute. Cyber attackers are using the connectivity to exploit widespread vulnerabilities in systems to conduct criminal activities, compromise information, and launch denial-of-service attacks that seriously disrupt legitimate operations.

Reported attacks against Internet systems are almost doubling each year and attack technology will evolve to support attacks that are even more virulent and damaging. Our current solutions are not keeping pace with the increased strength and speed

[1] National Research Council, *Computers at Risk: Safe Computing in the Information Age,* National Academy Press, 1991, recommendation 3c, p. 37.

of attacks, and our information infrastructures are at risk. Solutions are not simple, but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. However, we can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.
CERT©

Mr. THORNBERRY. Our final witness is Allan Paller, Director of Research at the SANS Institute of Cooperative Research, an organization that delivers education to people who secure and manage important information systems. As the others, we will include your full statement as part of the record, and you are now recognized to summarize it. Thank you again for being here.

STATEMENT OF ALLAN PALLER, DIRECTOR OF RESEARCH, THE SANS INSTITUTE

Mr. PALLER. Thank you, Mr. Chairman. It is an honor to be here, but I think we are even more thankful that someone of your insight and foresight is chairing this subcommittee. I am not sure the other witnesses here know that 6 months before September 11th, you actually put a bill in the hopper to form a Department of Homeland Security to bring together the Federal initiatives, and you spoke eloquently of the technical dimension. I am hoping that others get it earlier on this issue of cybersecurity than we all did on physical security and that we get the connections right; and with your partner here, Congresswoman Lofgren, who represents easily the highest concentration of security expertise anywhere in the world, and computer companies, and has shown real leadership on cyber issues—I think this could be a wonderful change in policymaking in government, and we are looking forward to it.

With that as an introduction, we at SANS train the system and network administrators—38,000 of them—on the front lines, and so we feel the pain when these attacks come. So my job is both to make some of what Bruce Schneier and Rich Pethia said real in terms of real-world examples, but also to say where we have succeeded and failed in trying to respond to them.

Five months ago today, we learned several big lessons with a new worm, the fastest one ever. It was called Slammer, and it was attacking machines—attacking addresses at the rate of 55 million every second, much faster than anything else had ever done. So from that worm, we learned several things. One is that we are in the middle of an arms race, that no matter how fast we build defenses, the attackers are going to continue to build attacks. So this isn't a war we are going to finish and get on with our lives. This is a war we are going to be fighting a long time.

The second lesson is that government and industry partnerships actually work. We talk about them all the time as if they are important, but this was a case where it absolutely worked. I have written the details in my statement. But very briefly, because the connections had already been established and the trust relationships were already in place between some of the leaders in homeland security and the private companies that are getting attacked,

there was instantaneous communication. They got together, got the word out fast enough, and protected a lot of people. So that was a very good example of where the public/private partnership can pay off and where homeland security certainly gets an 'A'. We also learned the limits to public/private partnerships, and I laid those out in my written testimony.

Another lesson we learned is that the physical infrastructure really is connected to the cyber structure. I am not sure if people believed that before. They thought, OK, cyber attack. So my Web site went out. Who cares? It is just kids, right? But in this attack, the Bank of America ATM machines stopped serving up money? If you had asked Bank of America before that event "Are your ATM machines connected to the Internet?", the answer was no, and yet they stopped. Continental Airlines couldn't schedule flights. Microsoft couldn't even get its XPs authorized. You use that service to register your new software. They couldn't do that because of the attack. And Seattle's 911 system stopped answering. This is the physical system. This is the critical infrastructure, and it is directly connected to the cyber network, and vulnerable to cyber attacks. So that was an education for us.

The fourth lesson that we learned, and I think the shocker, was that computer savvy organizations like Bank of America and Microsoft couldn't protect themselves. What Bruce and Rich were saying about the software being bad. It was so bad that the company that made the software that was being attacked Microsoft couldn't protect itself. So we are in a situation where users are getting software and hardware that is so hard to protect, that even the people who make it can't protect themselves. I think those lessons are useful.

The DHS provided some leadership in another area, and Congressman Turner pointed it out in a speech he made at CSIS, I think last week. This is a fascinating good thing that is happening, another 'A' for DHS. A consensus of a group of government agencies [the National Security Agency and NIST and DHS] and private companies, companies from Intel to Mrs. Field's Cookies are getting together to agree on what it means to have a safe system. That is important because if you don't agree on it, the vendors can't deliver it. If you have 50 people all arguing about what a sears system is, the vendors are stuck. Because of that user agreement, Dell was able to announce at the FTC hearings on June 4th—and Congressman Turner pointed this out publicly for the first time—that they would start delivering safely configured systems. We are hoping that is the first "Volvo". Remember, Volvo started delivering safe cars, and every other car company said, "Sure, if the public wants safe cars, we will start delivering safe cars." We are hoping that Dell's announcement is the beginning of a movement of vendors to start delivering systems that can be kept secure. It is going to be hard, as Rich pointed out. It is not a "3 weeks and we are done project," but it is a beginning.

You also asked a couple of other questions. You asked about losses from these attacks; and you asked how we measure them? In February of 2000, MafiaBoy attacked eBay and Yahoo and also took down CNN and Dell. I was the expert witness in the MafiaBoy trial in Canada, so I have more data about it than I otherwise

would. I saw the data about exactly what the victims said the attack cost them—it was confidential, but it went into the record. Remember that they were all hit exactly the same way. They were all down for about the same amount of time. They were all big organizations selling things on the Internet. So you would think that the estimates/damage would be nearly the same. They weren't. They ranged from zero to a few thousand dollars to one that said $5 million.

So when you try to estimate how much did this attack cost, which one are you going to use? Are you are going to multiply the number of companies attacked by 5 million or zero? Until we have a protocol for defining what we mean by the costs of an attack, we are not going to get answers that you are going to like.

One of the things you can do to help is to ask DHS to create such a protocol; how are we going to define the cost?

You also asked about simulations and exercises in your letter. We haven't done much in simulations, so we don't know how good they are. But we know exercises matter in this area of disaster recovery. In this very institution, a fire drill found that people turned the fire drill horns off in the computer room. So when the fire drill went off, nobody in the computer room did anything. You need to test emergency plans, or you will never know what is wrong.

The more important thing that can happen in tests is that mayors and governors, the first responders, would get to know the cyber people, and both groups would learn each other's needs a little bit, and they won't have to exchange cards after the attack comes. So I think the key benefit is that kind of sharing.

I want to close with a clarification of something that Bruce put in his written testimony—I was sort of hoping he would say it in his oral testimony so I could respond directly to it—but he didn't. In his statement he described an attack by Vitek Boden on the sewage system of Maroochy Shire in Australia. Boden got into the computer system. He changed the valve settings. He put back pressure on the sewage system, and human waste rose up in the streets of the city, like it does in your sink. People who lived there said it felt like they were living in a toilet. But Bruce pointed out that a bird landed on a transformer a few weeks later and did more damage than Vitek Boden had done, so we shouldn't think about cyber attacks as cyber terrorism. We are going to have much more likelihood of physical damage from terrorist attack than from a cyber attack. That is absolutely true. But the difference between Boden's attack and the bird's accident is the bird isn't sitting around planning how to automate the attack. The bird isn't sitting around loading up software, analyzing it. The bird isn't testing, deciding how much damage it can do. The bird doesn't want to hurt us.

We have seen, as you heard from the other witnesses, that the attacks are getting worse. They are getting worse at a rate of, I think close, to an order of magnitude each year and a half. The bird isn't getting that much better, but the Vitek Bodens of the world are getting that much better, and I think we ought to be ready.

Thank you for your time.

Mr. THORNBERRY. Lots of subject matter for further discussion, which I suspect we will get to.

[The statement of Mr. Paller follows:]

PREPARED STATEMENT OF ALAN PALLER

Chairman Thornberry, Congresswoman Lofgren, distinguished Members of the Committee, I appreciate the opportunity to appear before you today. It is particularly gratifying to us in the cybersecurity field, Mr. Chairman, that a person with your foresight, vision and leadership in homeland security has decided to take on the challenges of cybersecurity. I am not sure whether my colleagues are aware that six months before the September 11, 2001 attack, you introduced a bill in the House of Representatives that called for consolidating the federal agencies responsible for protecting our homeland. You saw the threat clearly; you spoke eloquently of the technological dimension, but it took a major attack before others were able to share your vision. I am very hopeful that in the cybersecurity field progress can be made more quickly. With your leadership and that of Congresswoman Lofgren, who has been one of the most effective Members of Congress on high tech issues and whose district includes one of the largest concentration of computer companies and cyber security expertise anywhere in the world, Congress can help the Department of Homeland Security lead a rapid effort to reduce this nation's vulnerability to cyber attacks, turn the tide against cyber attackers, and increase our speed and effectiveness in responding to and recovering from the attacks that do succeed.

My name is Alan Paller and I am director of research at the SANS Institute. SANS is an educational institution. Last year, more than 14,000 system administrators and computer security professionals, from nearly every government agency and large commercial organization in the US and from 42 other countries, spent a week or more in SANS immersion training. They learned the details of attacks that will likely be launched against them, learned how to build and manage defenses for those attacks, and learned how to respond once an attack has occurred. SANS 38,000 alumni are on the front lines in the fight against cyber attacks. Once they have returned to work, we continue to support them and more than 120,000 of their coworkers with early warnings of new attacks, weekly summaries of new vulnerabilities and a research program that makes available more than 1,400 timely security research briefs.

In 2001, SANS created the Internet Storm Center, a powerful tool for detecting rising Internet threats. Storm Center uses advanced data correlation and visualization techniques to analyze data collected from more than 2,000 firewalls and intrusion detection systems in dozens of countries. Experienced analysts constantly monitor the Storm Center data feeds and search for anomalies. When a threat is detected, the team immediately begins an extensive investigation to gauge the threat's severity and impact. Critical alerts are disseminated to the public via email and through the online press.

In my remarks today, I will share some of the successes and failures of the defensive community in responding to large cyber attacks, and I'll suggest ways that the lessons we learned might lead to effective initiatives for the Department of Homeland Security in improving response, recovery, and prevention.

Five months ago today, the Slammer worm attacked computers running Microsoft's widely used database management system. A worm, for those not steeped in the jargon of cyber security, is a malicious program that spreads from computer to computer without requiring users to take any action at all. Slammer represented a significant advance in attack technology. At its peak it was scanning 55,000,000 systems per second and that was 100 times as fast as Code Red scanned in July, 2001. Slammer infected 90% of the systems that were vulnerable in the first ten minutes of the attack and ultimately infected a total of 75,000 hosts. Slammer reminded the defensive community that we are engaged in an arms race with the attackers—one the attackers are likely to continue for many years. It did not contain a destructive payload; if it had thousands of organizations would have lost valuable data.

Slammer's high intensity scanning continued to wreak havoc for days. It surprised many people when it showed them that the computer systems that make up the nation's critical infrastructure for banking and transportation and emergency management - that some naively presumed to be somehow separate and isolated - are actually connected to the Internet and can be significantly affected by Internet attacks. For example, because of Slammer, Bank of America's ATM machines stopped dispensing money, Seattle's emergency 911 system stopped working, Continental Airlines had to cancel some flights because its electronic check-in system had problems, and Microsoft couldn't activate user licenses for Windows XP. Those were just a

sample of the more high profile problems. Many other organizations were damaged by Slammer, but they managed to stay out of the press. The cult of secrecy that surrounds cyber attacks is part of the challenge we face in determining costs and in helping people recover.

On a more positive note, Slammer brought our focus back to two valuable lessons. The first, learned in the summer of 2001 as we responded to the Code Red worm:

1. Federal and private security specialists, working together, can create a synergy that doesn't appear to exist when they act separately.

Slammer did a lot of damage, but it did much less damage than it would have if government and private industry had not worked together to fight it. A team of private sector experts from large internet service providers (ISPs) discovered the worm when it started flooding their networks. Within minutes they contacted technical experts in government and CERT/CC (Computer Emergency Response Team Coordination Center), and those three groups joined forces to analyze the problem. They learned that the worm targeted a specific entry point on each computer, and that they could stop most of the damage it was doing by blocking traffic to that entry point. The ISPs reconfigured their networks to stop all network traffic destined for the worm's target entry point, and their customers—at least the ones that did not have their own infected systems—stopped feeling the pain.

For Slammer, early discovery, effective analysis and widespread notification led to immediate extensive filtering of the worm traffic, and that action protected many organizations from being overwhelmed. This worked so well on Slammer that one might well ask why we do not use the same approach on all large, automated attacks. The answer is that two barriers get in the way and both can be eased by Department of Homeland Security initiatives.

The first barrier is that the high speed filtering used for Slammer does not work for many other attacks. Slammer exploited a special path that could be blocked easily by existing network routers, without harming valid traffic. The Code Red worm, on the other hand, exploited the path universally used to request web pages. Anyone who blocked that path would stop all web traffic to their site. For an organization that uses the web for business purposes, blocking that path could inflict more damage than the worm could cause. To filter for Code Red and other worms that use popular paths, the network infrastructure used by large companies and ISPs needs to be upgraded so that it can selectively block malicious traffic. That type of high-speed, intelligent filtering is not yet widely available from the network equipment manufacturers. The Department of Homeland Security could help speed the availability of high speed filtering routers through research support and targeted procurement.

The second barrier is that the government and the rest of the defensive community cannot respond to attacks if they do not know that attacks are occurring. Slammer flooded huge numbers of systems, so it was easy to find. Attacks aimed at electric power grids or e-commerce sites or emergency response networks are not nearly as visible. Early warning for targeted attacks is possible only if the first victims choose to report the attacks rapidly. But just as people infected with communicable diseases are loathe to make spectacles of themselves, so victims of cyber attacks can see insufficient benefit in making their pain public even to government officials who promise not to tell others.

How can we increase prompt reporting on cyber attacks? Let's take a closer look at the medical analogy. People who become sick, even with a highly communicable disease, do not usually call the Center for Disease Control. But their doctors do make the call, and the doctors maintain the confidentiality of their patients' identities. In the cyber defense arena, consulting companies serve as doctors to help companies analyze cyber attacks and recover from them. This year, the Department of Homeland Security (DHS) is spending millions of dollars to create a Cyber Warning Information Network (CWIN) that connects organizations active in cyber defense so they can get early access to important information. To ensure the "doctors" report attacks to the DHS, the Department could require that organizations that want access to CWIN must commit to providing immediate notification to DHS whenever they or one of their clients is attacked, without naming the victim.

Slammer also reminded us of another significant lesson we learned in responding to Code Red and Slapper and many other worms:

2. A severe shortage of individuals with technical security skills combined with a lack of management focus on security issues, prevents many organizations from fully recovering from attacks and improving their security. Better training is a partial solution, but joint action by government and industry to standardize security configurations and automate patching is already having a much larger impact.

Most attacks that do a lot of damage, like Slammer and Code Red, exploit vulnerabilities that are widely understood and for which remedies are known. Therefore it is surprising that two years after the Code Red worm swept through the Internet infecting vulnerable systems, 30,000 of those systems are still infected and still searching for other systems to infect. The problem is that many organizations that own computers have no one who understands how to secure those computers. When we find a Code Red infected system and ask why it hasn't been fixed, we usually hear that the system owner didn't know that it is attacking other systems and also that there is no one with security skills available to fix it.

Even large organizations are security-challenged. Slammer's victims included several huge security-sensitive organizations; Bank of America and Microsoft are examples. Their systems were flooded because vulnerable software had not been patched and because they had not configured their firewalls to block unwanted traffic from the Internet. It is unreasonable to blame the software users in this case, because Microsoft made installing this particular patch an arduous task, much more difficult than installing the underlying software in the first place. And most users and system administrators had never been told they should block the offending traffic at the firewall.

Training is part of the answer. Security-savvy system administrators are very effective at keeping their systems running smoothly while maintaining their defenses, and several large organizations are now requiring all system administrators to demonstrate their mastery of security as a prerequisite for getting control of the systems. However, most computers are not managed by system administrators. They are managed by busy people with other responsibilities. I do not believe it is fair or wise to expect that every graduate student or scientist or librarian who tries to install a workstation should become a security expert. And what about the grandparents and teenagers and all the other people who simply want their computers to work? We cannot ask them to develop and maintain the technical security skills needed to configure their systems safely and keep them secure.

A better solution is to remove the pain of security by centralizing and standardizing safe configuration and security patching. Large organizations can do that themselves, as the Department of Energy and others are demonstrating. But few other organizations have the time and talent. Only the companies that sell computers and software are positioned to make security configuration and patching inexpensive and effective.

Happily for all of us, vendors are beginning to recognize that security is a critical market need, and they are putting their development dollars to work to help their clients with security. Three weeks ago at a Federal Trade Commission workshop, Dell announced it would sell Windows 2000 systems configured in accordance with consensus security benchmarks, improving security and reducing the security burden for Dell customers. Similarly, Oracle and the Department of Energy are partnering to deliver safe configurations of Oracle software to all users at all Department of Energy laboratories and offices. Other Oracle users will benefit as Oracle makes the safer version available to the general public. Both of these efforts were facilitated by an extraordinary public-private partnership involving the National Security Agency, the Defense Information Systems Agency, the Department of Energy, NIST, FedCIRC, SANS, and the Center for Internet Security (CIS). The CIS partnership has developed consensus benchmarks for safe configuration of many common operating systems and applications. Dell, for example, said that they would not have been able to create the new safer version of Windows 2000 without the work of the CIS partnership.

And automated patch delivery is maturing. For example, Red Hat delivers security updates for its software automatically as does Microsoft for some its Windows XP software.

It is common practice today for vendors to sell software and hardware with insecure configurations. Most users are not security experts and therefore are not aware of the configuration dangers, nor do they have the knowledge to find and apply appropriate security patches. All that means that millions of computers are at risk, and each of those vulnerable systems can be used by attackers to launch major denial of service attacks. With active leadership by the vendors and the federal government, worms and automated attacks will be denied easy access to all these systems.

So what can the Department of Homeland Security do to accelerate this beneficial trend? DHS can require its vendors to deliver safe systems out of the box and ensure that patches are delivered automatically. As other federal agencies and companies follow the DHS lead, the market will reward vendors that take security burdens off their customers' shoulders.

In your letter of invitation, you also asked me to address the challenges in estimating the damage done by cyber attacks and the strengths and weaknesses of simulations and exercises for cyber security. I'll answer both briefly because the general knowledge base about both is limited.

How Much Do Cyber Attacks Cost The Victims?

In the MafiaBoy denial of service attack on eBay, Yahoo, Dell and several other marquee web sites in February of 2000, each victim confidentially reported its actual losses to the FBI. I know a little about that case because I was the expert witness for the prosecution in MafiaBoy's trial. The technical attack on each victim was basically identical, and the outages were roughly the same length, but victims reported radically different estimates of damage. Their estimates ranged from zero to $5,000,000 depending on whether they included lost revenue, damage to reputation, management time, the direct costs of staff involved in the investigation and recovery, or none of those. Estimating losses is much more of an art than a science.

Another example of the difficulty of estimating losses was illustrated by the Nimda worm that raged through the Internet seven days, nearly to the minute, after the first airliner crashed into the World Trade Center. I interviewed more than a dozen victims confidentially, and they consistently told me the damage they incurred was between $300 and $700 per system—the actual cost of removing the infections from the systems and reinstalling software and data. For 150,000 infected systems, that adds up to about $75 million dollars. Yet within days of the attack, an economics firm was telling the press that the price tag was $835 million. Other people gave estimates exceeding $2 billion. Before policy makers can rely on any damage assessments, a common protocol for damage estimation is needed. DHS can help develop that protocol.

How Important Are Simulations and Exercises?

Simulations and exercises are both valuable for improving America's effectiveness in responding to cyber attacks. The mathematical models simulating worms, created by organizations like CAIDA (Cooperative Association for Internet Data Analysis) at the University of California's San Diego Supercomputer Center, were instrumental in giving policy makers effective projections of the numbers of systems that would ultimately be infected by various worms. That kind of knowledge is extraordinarily valuable in the pressure cooker atmosphere of a worm infestation.

Simulating attacks through real world exercises are just as important for two reasons. The first reason is that emergency response systems rarely work as they were designed to operate. A few months ago a past deputy director of the House Information Systems (now called House Information Resource) told me a story about an exercise testing their fire emergency response plans. He wanted to ensure his organization would respond appropriately if a fire broke out in the building, so he scheduled a fire drill. When the alarm went off, most people, following patterns most of us developed in grade school, left, but no one in the computer room reacted at all. In a real fire they would probably have died. The problem: for some reason, in wiring the computer room, the electricians disconnected the power to the horns that sounded alarms. The computer room staff never heard the alarm. Without an exercise, no one would have known.

The other reason to run exercises involves the cyber dimension of physical attacks. Recall that in the aftermath of the September 11 attack, not only buildings were destroyed. The networks and systems of the New York Stock Exchange and all of Wall Street were a shambles. Without rapid reconstitution, the negative economic impact of the September 11 attack would have been even greater than it was. Verizon staff worked with the city's leaders 24 hours a day every day to rebuild the telephone and cyber networks needed to get trading restarted on Wall Street. They did an extraordinary job under difficult conditions, and a substantial part of their success was made possible because Verizon had already built a strong relationship with the mayor's office and the emergency response teams through planning and exercising disaster recovery protocols. Most cyber teams have no such connection with first responders and they need to know one another before an incident occurs..

We cannot have those groups exchanging business cards after an attack. The first responders will do a better job of planning if they know the cyber experts who can help them recover their networks and the issues those people will face when responding to emergencies. At the same time, the cyber people will be better team members if they understand what the mayors and governors need and jointly develop the action plans. We need to give the cyber people a seat at the table when planning for emergencies. These groups should learn from each other in advance, test communication paths and their ability to work together, identify problems and potential solutions, learn how long things take and how to speed them up. Exercises are the best way to make that happen.

What Can DHS Do?

Finally, you asked about how the Department of Homeland Security should work with the private sector in improving response and recovery. Let me summarize two key suggestions that go beyond the recommendations I covered earlier:

1. A central goal of the Department's cyber initiative should be to provide a single, technically savvy coordination point that the experts can rally around in responding to major attacks. I have been extremely impressed by the quality of people the Department has recruited to set up and run the new Cyber Security Tracking, Analysis, & Response Center (CSTARC). That group proved it can do extraordinary work in bringing together the public and private sector, both in responding to a vulnerability in sendmail and in the Slammer worm response. The key to CSTARC's long-term success is establishing a core group of very skilled people who then build a network of experts inside and outside government. Through exercises and responding to actual attacks, this community of cyber first-responders can create protocols and allocate responsibility for isolating malicious code, analyzing it, developing automated diagnostic and repair tools, and disseminating the tools and knowledge to the right people very rapidly.

2. As important as response and recovery are, prevention should have equal priority. DHS should allocate a large share of its time, attention, and budget to reducing the cyber vulnerabilities this nation faces. DHS can help by encouraging and supporting development of consensus benchmarks for safer configurations, but the Department's greatest impact on vulnerability reduction will come from persuading vendors of software, hardware, and network services that the government is serious about buying and running safer systems. The federal government is the only buyer large enough to get the attention of big vendors. DHS should make it clear, through both talk and action, that success in selling to the federal government is contingent upon delivering safely configured systems and automating the process of keeping those systems secure over time.

Thank you again for inviting me today and for your leadership in holding these hearings. I would be happy to try to answer any questions you might have.

Mr. THORNBERRY. Let me reserve my questions and turn to Chairman Boehlert.

Mr. BOEHLERT. I thank all the witnesses for serving as resources. I really appreciate it. We have got a lot to learn. I am reminded of the story of the guy looking at his house burning down who turned around and said to the first person he saw, Where do I buy a fire extinguisher?

I would agree with your analysis on the Chairman. He gets it. My concern is not enough people get it in positions of responsibility. I think we are beginning to get it, and it is appropriate that we have this meeting in this room, the Science Committee room, because in January of 2001 we introduced the Cybersecurity Research and Development Act, a very significant undertaking calling for the authorization of a lot of money, hundreds of millions of dollars, at a time when we are struggling to keep the budget balanced.

But quite frankly the response, except for people who get it—and Mr. Smith right next to me gets it—the response was a muffled yawn; oh, we have got other things, bigger items on our agenda. 9/11 came. Then the House passed this new multimillion dollar—hundred million dollar authorization by a vote of, like, 400 to 12. There were 12 that still don't get it.

So now we have this Cybersecurity Research and Development Act. We now have an agency with responsibility for coordinating the cybersecurity efforts of the Federal Government, the National Science Foundation. We have NIST engaged. DHS is engaged.

My question is, do you think enough people in this town get it? I know the President does. He couldn't add his signature fast enough to that legislation that we passed, but still we had these

massive authorizations, and the appropriations that are following are minimal.

And Dr. McCrery over at DHS, I mean, part of the education process with him, the new Under Secretary for Research and Development, they have got to devote more resources to cybersecurity, because you can't build a building on the tenth floor. You have got to start with the foundation. We don't have students in our great universities with advanced-degree capability dealing with cybersecurity. There are a whole lot of problems. Do you think that people in this town are beginning to get it? Not fast enough, but beginning to get it?

Mr. PALLER. I get asked frequently "How can I get the President of my company to pay attention to security?" It happens often. I had two speeches yesterday and it came up in both of the speeches.

Executives get it, but they don't internalize it, because it hasn't touched them where they live yet. As soon as it does, as soon as it touches them, everything changes, just the way everything changed after 9/11. So, no, I don't think this town gets it, and I don't think argument is going to get them there. I wish it would. I wish this kind of publicity would do it, but I think it is events that educate people. I do think we need to educate them about the events. Too few people know about that Slammer worm and how much damage it did to the Seattle 911 system. I think we need to teach them so that they feel the events are real. But, no, I don't think most people feel internally that cyber threats matter to them at least not enough to invest in effective defenses.

Mr. BOEHLERT. So many people think in terms of cybersecurity and they think they want to protect themselves against some brilliant 15-year-old hacker, but it is so much more than that. Quite frankly, I don't think it is far-fetched. It is not stuff of Buck Rogers to suggest that the next war could likely be fought without bullets and guns. It could be fought on computers.

Mr. PALLER. There is no question that our nuclear systems, that our electrical systems, that our infrastructure can be attacked through cyber means.

Mr. BOEHLERT. The whole economy is dependent on it.

Mr. PALLER. And our banking system. But persuading people of that when it hasn't happened to them yet is just very difficult.

Mr. BOEHLERT. You are a student. You watch what is happening in this arena, particularly in areas of assigned responsibility. Now, do you feel that under this new Cybersecurity Research and Development Act, the Federal Government is moving in the right direction with having a coordinated source of responsibility—the National Science Foundation for the R&D part of the effort and the education part of the effort—because if we don't train more people who have more knowledge about this subject and get them in positions of responsibility, we are still going to take a ho-hum attitude.

Mr. PALLER. That bill was wonderful, and Carl Land over at NSF is doing a great job at concentrating the funds. The money you are spending on training students is very effective, but—appropriations are tiny, so we haven't yet seen how much good that money can do.

Mr. BOEHLERT. Well, you are preaching to the choir here, because we are all going to push for a lot more appropriations.

Now, part of the problem has been—I remember talking a few years ago to a high official of a major credit card company, and he casually dropped the thought that they lose about $100 million a year to fraud and abuse, and he said, But they view that as an acceptable loss because it would cost them more than 100 million to prevent the $100 million loss.

Well, I think that thinking is changing. But the problem has been and the whole industry's effort has been to get a product to the market that is faster and cheaper, and security hasn't even been factored in. Do you see any trend changes that customers are demanding that security be built into the product and—for example, like I am demanding that I have air bags in my car and seat belts, and am willing to pay a couple bucks more for it. Do you see the market changing?

Mr. PALLER. Yes.

Mr. SCHNEIER. I don't very much, unfortunately. And the problem is—I mean, I can hold two products; one is secure and one isn't. They use the same marketing speak, the same words. You, the consumer, can't tell the difference, and customers are just as happy with promises of security than reality as security. There is not much difference. And what I find—and this is—I am struggling with this. I mean, there are lots of great products. The average firewall out there is not installed properly. You know, good software design practices are not being followed. I mean, we have a lot of things we could do we are not doing. Policy, no one has a good policy. They exist. We can do this, but companies don't seem to be getting the message.

Slammer is a great example. It did lots of damage, all sorts of things. The average CEO never heard of it. It didn't affect him. Your comment on Visa I think is perfect. Visa is saying, "Look, we have these millions of dollars of losses it will cost us more to fix than to eat." That is a perfectly rational thing for a business to do. You have a risk. You either fix it or accept it, depending on the value. Maybe you insure it if that is cheaper.

And so my problem is not the technologies. There are technologies. Technologies can improve. Education is great, but unless there is a pull, unless businesses have it in their best interest to produce this secure software, to build secure networks, they are just not going to do it. They are going to say, like Visa, you know, the losses are not great enough. But if possible, there were criminal penalties, if there were liabilities for identity theft, if the losses were greater because of whatever government mechanisms we like—and depending on your politics, you pick different mechanisms. It doesn't matter which ones you pick. If we raise the penalties, then the cost of fixing becomes comparatively cheaper and more companies will—Visa will say, hey, we are going to improve our security, because now it is cheaper than letting it go, because the penalties of letting it go are greater.

To me, the business process is broken. It is not the tech.

Mr. THORNBERRY. The gentleman from New Jersey, Mr. Andrews.

Mr. ANDREWS. Thank you, Mr. Chairman. I would like to thank each of the three witnesses for outstanding and substantive testimony that has really added a lot to this discussion.

Mr. Schneier, I wanted to talk to you about your conclusions about what I believe you characterized as an exaggeration of the threat of cyber terrorism, if I read your articles correctly. I agree with you that the ability to use the Internet as a tool of murder, a tool of death, is fictional, largely fictional. It may happen someday, but it is largely fictional. Our concern, though, tends to be a coordinated attack.

I notice in your June 15th article, in the second paragraph, you say: The software systems controlling our Nation's infrastructure are filled with vulnerabilities. Our concern, frankly, would be a coordinated terrorist attack where, for example, the telecommunications system would be compromised in a city where simultaneously four or five explosions might occur which would disable people from calling the police, calling the ambulance, and so forth.

And then the third is secondary-level response, would be the economic damage that will be done to the economy of that area. Do you agree that that is a viable threat?

Mr. SCHNEIER. It definitely is. You think of 9/11, that is what happened. The World Trade Center fell on top of most of the telecommunications infrastructure of lower Manhattan. So we see that, and, you know, I would give—if I were a terrorist and reasonably clever, I would think of those sorts of things. So for me, the cyber part is sort of in the noise—I mean, when you fly a plane into a building, making people's phones not work is kind of like the extra candles on the cake.

Mr. ANDREWS. Of course our concern is not that they would fly into the building and make someone's phones not work, but that they would find a way through the cyberspace to make the phones not work and then couple that with a series of fairly low-tech physical attacks that would create chaos and panic and economic dislocation. Do you think that is a viable scenario?

Mr. SCHNEIER. I think it is definitely worth worrying about. And remember, attacks are getting worse. We are all saying that. So even if I say, Look, it can't happen today, call me back in 18 months and I will say, my God, this is a problem.

Mr. ANDREWS. One of the common problems I saw from each of you was the government's use of purchasing power to raise standards of the cyber wall, if you will. I think Mr. Boehlert has done an extraordinarily good job by taking care of the research piece in the legislation that he got enacted last year. I think we are deficient in the use of that purchasing leverage, as well as we should. I have enormous faith in the private sector of this country in this area. I think this is one area where the private firms, the small ones and the large ones, the Microsofts and the ones we don't know the names of, have done an extraordinary job in providing technological solutions. And I think Mr. Schneier said a few minutes ago it is a business problem, not a technological problem, to make those solutions even more viable.

How would each of the three of you suggest that we reorder the Federal Government's purchasing specifications and use of purchasing leverage so as to enhance cyber protection for the critical infrastructure providers not in the governmental section? To put it in plain English—and then I will stop—is how can we increase the quality and lower the price of a protective product that Verizon

could buy or that the people who run the power grid could buy so they could make us more protected?

Mr. Paller, would you like to start with that?

Mr. PALLER. Sure. I actually see change in procurement happening right now. You will hear an announcement in the next few weeks that the Department of Energy just awarded a huge contract to Oracle, and in it they required Oracle to deliver a safely configured version of Oracle's database software. Oracle agree to it because DOE had a lot of money to spend, and what made it possible was this consortium I talked about, and Congressman Turner talked about, that has created standards, benchmarks, so that DOE could order software with those benchmarks.

The key fact here is that, when I mentioned the DOE contract to the CIO at Justice, who is also the chairman of the CIO Security Committee, his ears perked up, and he said, I have got to get on that.

The hunger to use procurement for improved security is there. The actions of the vendors are not quite there yet. They honestly say "We can't do that until you guys agree on what you mean by 'safer,'" and that agreement is what NSA and NIST and DHS have been taking a lead in creating. Once you get that kind of leadership, I think you will find that the buyers are hungry for safer systems and will use procurement to get them.

Mr. ANDREWS. So you see our role as setting viable and constantly improving technological standards that the market will meet if we set those standards correctly?

Mr. PALLER. I see your role as encouraging the industry and government to work together to do that.

Mr. ANDREWS. To do that, not to buy products that don't meet those standards for our own use. Correct?

Mr. PALLER. Yes.

Mr. ANDREWS. Mr. Pethia.

Mr. PETHIA. I think—I have two parts to the solution from the way I see it. First of all, the idea of standards I think is exactly on track. The problem with standards is the devil is always in the details, and trying to have a set of standards that actually demonstrate improved security is sometimes hard.

So I think in the short term there are obvious kinds of product problems we know about. We have seen them year after year after year after year. We know about configuration weaknesses. We know about certain kind of coding errors. We know about certain kinds of testing problems. Simply setting a set of standards to deal with that class of problem alone I think is one step that takes us a long way towards a solution, and in fact we will probably get rid of about 80 percent of the vulnerabilities that we see out there.

Once we go beyond that, however, we are going to find that the attackers will understand how to attack even those more secure systems, and that second step requires additional research, because we don't know how to build—.

Mr. ANDREWS. My time is up. Thank you.

Mr. Schneier, if you want to—then my time is up.

Mr. SCHNEIER. If you are a Fortune 500 company, you would standardize in a few good products, you would write yourself a really good purchase order and demand features that you want.

That is what you should do. The devils are in the details, but you guys are a consumer of security. Unlike a lot of other areas of security, your problems are industry's problems. It is the same threats, the same attack tools, same hackers. So everything you do immediately benefits us. It is not like you are buying a missile, where it is all your requirements and we don't care.

So I would like you to—I mean, with the help of whoever—develop purchase orders, develop specifications that meet your security needs, and demand them. I mean, you are going to buy a whole lot of products, and companies will meet them. I agree industry can do this if there is demand, and once you do, they are going to offer those same products to us. They are not stupid.

Mr. ANDREWS. Thank you very much.

Mr. THORNBERRY. Thank the gentleman.

The gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Let me address my first question, I believe, to Mr. Schneier and Mr. Pethia, and this is a question that really comes from a number of meetings that I have had with constituent high-tech companies. I represent literally hundreds of high-tech firms and basically they tell me what I also hear here in Washington at various briefings, and that is that a cyber attack in some shape or form, which we know had been occurring, are going to continue to occur and inevitably they are going to be successful or semi-successful one way or the other. Also, as we know, a cyber attack using cyberspace might be in conjunction with a more conventional type of attack as well.

But my point is this: They think we will be—that an attack will be successful. We don't know whether yet it is going to be planting viruses in computers, disabling energy grids in California or Texas or wherever, but their point is that we have the technology available now, and in many many cases these individual high-tech companies are giving the examples of that kind of—those kinds of solutions, but that the government is not yet taking advantage of the high-tech solutions that are available right now.

And I would like for you all to address really two questions. One, to follow up on Mr. Andrews' questions, what kind of attack do you think is most likely? And, two, do we have the capability to defend ourselves against it? And if not or if so, are we using all the high-tech kind of solutions that are available to the best of our ability?

Mr. PETHIA. A likely attack, I don't know how to predict, other than the one lesson I think I learned from 9/11 is that we have an adversary who is patient, who is willing to do homework, who will do surveillance, who will find weaknesses, and wherever those weaknesses are that they think they can get the biggest benefit of, they will take advantage of. But I don't know how to predict human behavior beyond that, but I think it is going to happen someday.

As far as do we have the technologies we need to protect ourselves, the answer is yes and no, unfortunately. Today if you are a very capable system operator and you are willing to invest a lot of time and money and you are willing to do things like install firewalls, intrusion detection systems, authentication devices, one-time password technology, use encryption in the right way, et cetera, et

cetera, et cetera, then, yes, you can do a good job of protecting your systems. So that part of the answer is yes.

But when you put all that together and understand how expensive it is and how complicated it is and understand that any mistake in that whole configuration at any point can make your systems as vulnerable as if you hadn't done anything, then the answer, unfortunately, is no.

But we can secure our systems, but the problem is today it is just too hard and it is just too expensive.

Mr. SMITH. Mr. Schneier.

Mr. SCHNEIER. I agree with all of that. The great military strategist von Clausewitz would call this a position of the interior. All right. The defender is a unit, and he has to defend against every possible attack. The attacker just has to find one way in, one weakness. So in that way, the defender is at an enormous disadvantage.

All right. The attack that is likely to come is the attack you didn't defend against, right? Because if I am the attacker, I am not going to attack you where you are defended. So sort of by definition, there are going to be weaknesses. Unless you defend against absolutely everything, right, there will always be a weak link.

I would assume the kind of attacks that are coming are the kinds of attacks you have already seen and then the new ones you haven't seen yet. They are going to be all over the map. We probably have the ability to defend against some of them. These comments were really dead on. I mean, yes, you can—all right. If you took your computer and you turned it off and buried it underground, no one could attack it, but it is not terribly useful. Essentially by the very fact of we are using our infrastructure, we make it vulnerable. Right.

Your house would be more secure if there were no door, but you need to put a door in. Therefore, there are insecurities. You can put a lock on your door, now there are all sorts of problems.

Are we doing everything we can? Of course not. Because everything we can doesn't make any sense to do. There is always going to be a balance. Right. What is the risk, and then how do we defend against it rationally? And depending on who makes that balance, you are going to see different sorts of things. Right.

The shed in my backyard doesn't have the same lock as my front door. The risks are really different. And this is where I sort of talk about making the risks—getting the equation right. A lot of the risks we are facing are residual risks. They are not risks that the companies are facing. So they are going to look at a lot of these measures, that great laundry list, and say that is too expensive, too complicated. We don't have that kind of risk. They don't. But we as a Nation do, and that is what scares me.

Mr. SMITH. Thank you for your answers on a complicated subject. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

And let me thank each of you for being here today. This is not only very important but very instructive. Let me follow that line, but in just a little different way; because on the first hearing, the Chairman will remember, I asked a question about a number of

our software now—because we are dealing with international companies—is done overseas. So in my State and nearly across the country now, we have talked a little bit about banks and others, because they are hiring a lot of foreign firms to write software for the businesses. But recently several banking firms have been instructed by their security specialists to start advising financial institutions to certify the integrity of the software that is written overseas, as you can appreciate.

But me question is this: Do you believe software sabotage is a real threat? And number two, how will a company check the software to ensure the integrity of it? Who wants to tackle that one?

Mr. PETHIA. I think the problem of malicious code embedded in software is a real problem, and I don't know that offshore has anything to do with it. I think we have bad guys here as well as offshore. The big problem, however, is detecting that malicious code, and frankly, we don't have good ways to do that.

Even in cases where the source code of the software is available—and often it isn't—even there it is very difficult to take a huge application, which may have literally millions and millions and millions of lines of code, and find the 20 or 30 that cause some back door to open to let the bad guy do what he will do. So that is another area where I think we need a lot of research that helps us understand how to build software that is free of these kind of defects, or if they are there, that they can be detected. Frankly, the industry or the academic community doesn't know how to do that now.

Mr. SCHNEIER. Well, and luckily you get virulent agreement among the panel here. Everything you said is right. I don't think international makes it worse, although you can certainly imagine a concerted effort. I don't know, I am not impressed by that. We see a lot of sabotage for personal gain, for extortion. I mean, I can mail you dozens of real criminal cases. He is right. It is very hard to detect this.

In a former life, I used to do consulting where I would look at source code, and I would tell companies, figure you should spend as much on evaluation as you spend on development. Now, of course, companies are never going to do that. It is just too much. But that is the sort of thing you have to think about. And when you look at, you know, sort of high-risk code—now, code in Boeing aircraft, some code that the military does, maybe for nuclear launch codes—they do that. They will spend as much money on security and safety testing as they do on every other aspect of the project, because it is really important for them.

Now we are sort of entering a world where every bit of code is slowly becoming that important; and, no, they are not ready to deal with that. That is going to be a big deal, and it is definitely worthy of concern.

Less from the, you know, I am going to take down the Internet and I think more crime. Again, I think the risk of cyber terrorism is overstated, and we grossly underestimate the risks of cyber crime. We are seeing a lot more crime on the Net. So when I look at these attacks, I am worried about the ones that are criminally motivated, I am going to put something in the code, and then I am

going to call the company and say, hey, give me a million dollars and I will tell you where it is. That kind of thing has been done.

Mr. ETHERIDGE. Let me follow that up, because you indicated you touched on this earlier, that the statistics indicate that about 80 percent of the critical cyber infrastructure is in private hands. And I think in most of the testimony of almost all three of you, you had suggested that how you work on that is to encourage software vendors to create better products, and that is really what we are about. And would you expand just a little bit more? You touched on it earlier about what the Federal Government can do.

Mr. SCHNEIER. It is two things. We need to encourage software vendors to produce better products. Then on the demand end, we need to encourage the consumers of those products to use them securely. I mean, there are lots of secure products that nobody is buying. And there are lots of insecure products that everyone is buying. And the problem—the reason we are here is because it is not in the best financial interest of either the software vendors or the network owners to increase their security.

Mr. ETHERIDGE. Let me follow it up, because I think this is critical. If there were—let's say I go out and buy a piece of equipment for my home. There is no coding today, whether I use that in my home or whether I use it in business or if I am with one of the largest banks, but if there were a code attached to it like a 1, 2, 3 to indicate a level of security or something on it, as you do with some other things, is that the kind of thing you are talking about would have an impact?

Mr. SCHNEIER. Well, I mean, completely finessing how you would get that code, I mean, magically there and magically accurate—I mean, that would at least provide some indication of quality.

You know, what I want to see are the business processes getting involved. As a security guy, I can talk with a security person who says, yes, I am desperate for more security but when I go to my CEO or CFO they say the risk isn't that great, it is cheaper for us to ignore it than to fix it.

Well, that is because the risk is primarily in other people's hands. If I am a company that owns a big database of credit card numbers, if it is stolen, if there is identity theft, it is not my problem. It is the problem of the people whose identity was stolen. So I am not going to protect it to the degree of the sum of the individual risk of my customers, because it is not my risk.

And, I mean, there are several ways we have dealt with this in other areas of society. You know, in environmentalism, we passed some regulations. We have used some economic incentives. In things like automobile security, we have liability laws. We have also changed public perception so that air bags are considered a good thing. All right, that was the industry itself using security as a marketing tool. All right. That also works. Changes in technology work. If you—if there is a door—a good example, our alarm systems. When they became wireless, they became a lot more prevalent, because they were cheaper and easier to install. So as policymakers, you have several levers. All right. You can deal with the regulation liabilities. You can deal with putting money into technology and making that better. You can deal with social norms.

All right. You get to choose what levers you pull, and what the levers do is, they affect the business motivations, which then act both the supply, producing secure software, and the demand, wanting secure software.

Mr. ETHERIDGE. Thank you.

Mr. THORNBERRY. Thank the gentleman.

The gentleman from Nevada, Mr. Gibbons.

Mr. GIBBONS. Thank you very much, Mr. Chairman.

And to our witnesses let me express my thanks as well, as my colleagues have done, for your presence here today and the testimony you have provided us. As I sit here, I have to admit that I am probably one of the few people on this panel who is not very well educated in computer technology, and it is an evolutionary process in my own mind to get my arms around it to understand a lot of this. And I presume that is pretty a much widespread problem with the American public today. They know a little bit about it but not a lot.

The evolution of technology that is occurring in the computer industry is so rapid. Do we really have a real expectation that what we create today will be an answer for a 15-year-old's bright inquisitive effort to break it tomorrow? Are you comfortable with what you are saying today is the protection and the security that we can create, will give us the real barrier that we need to some mass disruption, some mass attack? Anybody want to take that on? I mean, it is a hypothetical.

Mr. PALLER. My sense is that we can remove the vast majority of the easy ways to break into our systems. Rich said about 80 percent of the attacks—used well-known vulnerabilities. We can wipe those out. We are not yet wiping those out, and we have to do so right away, and that raises the bar.

Next the research money that Chairman Boehlert was talking about has to be invested to find better ways of testing the code, of building more secure systems; but if we wait until we build the better systems, then we are simply leaving all of the doors and windows open and just saying to the attackers, "come get us."

Mr. GIBBONS. Well, then, Mr. Schneier, let me ask you a question; because if that is an answer that we have got to develop the research to provide for the capability of presenting the real serious or in-depth attack that we just talked about, are our universities providing a level of expertise and resources capable of being able to do that, or are our universities falling short in educating people?

Mr. SCHNEIER. Some are. There is some great research being done, some great education being done. It is not enough. The demand for computer security far outstrips supply. If you know any kids who are going into computers, tell them security is a whole way to make a whole lot of money, because there is a lot of demand for jobs, and there is great research out there, phenomenal work.

CERT is an institution coming out of Carnegie Mellon. They have been doing phenomenal stuff since forever. You have to look at it as two different attacks, and what Alan was saying is exactly right. Most criminals are opportunists. They are getting a tool and using it. Most vulnerabilities being exploited are the obvious dumb ones.

So security is an arms race against professionals, all right, the people out to do real damage. Most of the attacks are low level—

it is low-hanging fruit. We can do a lot to get rid of that and that really does raise the bar. After we have done that, we have still got the arms race, and that is never going away; because you are right, you know, defense now, new attack, new defense, new attack, it is going to get worse. But the last thing we want is for all the old attacks to work as well as the new attacks.

Mr. SCHNEIER. I sit at Counterpane. We monitor companies, we monitor vulnerabilities, and the hardest thing we have is to get rid of the kids attacking and trying to find the real attacks.

Mr. GIBBONS. Well, if we do have the capability today and if we do have the resources that would allow for someone to attempt or succeed in a mass disruption of our information technology systems around the country or in any community, why have we not seen a major effort in this regard so far from the terrorist side? Not from our defensive side. Why have we not seen a terrorist really try this so far? Because we all we see today are the criminal-minded hackers.

Mr. SCHNEIER. I have written about this. I believe the answer is it is not terrorism. Sort of imagine Bin Laden sitting in his cave plotting the next attack against America, and he is not going to say, "I know, let's disrupt their chat rooms." He is not going to say that.

He is going to say, "Let's kill a lot of people, let's cause mayhem, let's cause terror."

The Internet is important, but it is—it doesn't put bloody bodies on the front page of a paper, which if you are a terrorist is what you want to do. Eventually it might, but today, a terrorist is not—I don't see it as a way to cause terror.

Mr. GIBBONS. If he interrupts our business systems, the economy of this country is probably as critically important to the lives and well-being of everybody in this Nation as anything we can think about today.

You interrupt the food supply, you interrupt the communications capability, people can't call a hospital, can't get an ambulance, you interrupt their ability to go to the store, that is as much a terrorist act as flying a plane into a building.

Mr. SCHNEIER. But it is harder than you think. When the phone system went down in New York City after 9/11, people picked up their cell phones, people used their pagers. There are a lot of networks that got up in a few days.

Our infrastructure, even though vulnerable, is surprisingly resilient. You see bad effects. The strike on the West Coast closed the ports and had monstrous effects on American industry. That wasn't terrorism, that was labor relations. And, yes, an attack like that would cause those effects.

But, to me, and I am just trying to put myself in a terrorist mind-set, it doesn't feel like the best bang for my buck. Maybe it is, and maybe we have just been lucky and that is another way to look at it. Eventually someone is going to think exactly along your lines and do it. I mean, the question is not if, the question is when, and maybe it will be something we can recover in a few days, maybe it will be something we can't recover and businesses that require the Internet will go out of business for a month.

It is very hard to speculate. We all agree here that the problem is getting worse. So if we are talking about 5 or 10 years, certainly I think everything you are thinking gets a lot more reasonable and a lot more likely.

One more point I want to make based on your first comment. I actually have a book I am going to hand out. This hearing has homework. So I got a copy of this for all you guys, and you can either read it or give it somebody else to read. But I did a book sort of on computer security, and a lot of things we are talking about here, how to understand the issues. My mother read it, so don't be scared.

Mr. ANDREWS. Mr. Chairman, this is a flagrant violation of the rules of Congress, to ask us questions and give us things to do. This is outrageous.

Mr. SCHNEIER. No one said you can't give homework.

Mr. GIBBONS. Well, gentlemen, thank you very much for your expertise. And thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentleman.

My response is we need all the help we can get from whatever source.

The gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Mr. Chairman, most of my questions have been answered. I am going to submit some questions for the record, but I will yield at this time.

Mr. THORNBERRY. The Chair thanks the gentleman.

The gentleman from Texas, Mr. Sessions, vice chairman of the subcommittee.

Mr. SESSIONS. Thank you, Mr. Chairman, and I want to thank you for not only planning, but putting together, what is a very interesting hearing today.

I would like to switch gears a little bit, if I can, and go to what would be the bottom bullet for each one of your testimonies and focus, if I can, for half a second on the attacker, who is the attacker, what is that level of sophistication?

The second part of the question is how it is reported to law enforcement, what are those piece parts towards trying to catch the attacker?

Lastly, in that chain, success in working together to identify the real threats versus what was said, to get rid of the kids, to get the kid stuff out of the way for the real attack.

I am interested in this chain of information. I think from a primary aspect of business, identification, working with law enforcement, successful prosecution, I am interested in that summarization from any one of you.

Mr. PALLER. Two things. One is the FBI has gotten extraordinarily good at catching some of these people. The ones they catch are the ones who do stupid things like brag, however. So we are seeing lots and lots of successes, putting people in jail, and they are going to jail for longer periods of time.

When you ask who these people, Mafia Boy, for example, was a very angry, person what teachers would call a rotten kid—who did a lot of damage independent of his cyber work. When he got cyber tools, he went after E-Bay and Yahoo! and took them all down. It was part of acting out as a bad kid, but it did a lot of damage.

What we don't know is who the people are who will do the really complex attacks. Because we don't know who they are, we actually have to build the defenses with more vigor than we would if we could identify the attackers' targets and take them out. That is why this problem is so difficult, because they could be everywhere attacking us.

I can offer answers to the other questions, but I will let other people speak.

Mr. SESSIONS. Does that mean it could be across the world, it could start someplace and go to another, and go to 10 places before it actually was able to be seen and we just can't figure out the chain?

Mr. PALLER. I didn't mean that. I meant it could be a group of terrorists in Indonesia that right now is shooting guns at people and figures out a way to get some money and uses that money to hire some hackers who don't know that they are being used by terrorist. We just don't know who they could be. Even the smart hackers can be fooled into working for the bad guys. They don't know who they are working for. Somebody claims to be from the NSA, how does a hacker know he is not? We don't have a clue where the attackers are. That is why we have to build the walls so strong, instead of saying "Let's go get those bad guys and take them out."

Mr. SCHNEIER. Chapter 4 talks about who the attackers are.

Mr. SESSIONS. I will read my homework.

Mr. SCHNEIER. They range from the kids to foreign governments who are going to use cyberspace as a theater for war, which is a perfectly reasonable thing. We do that kind of thing in our warfare. It would be crazy to assume that somebody won't. They are all over the map.

How is it reported? Largely it isn't. This is where you start to think about what are the risks. There are the direct losses, the loss of whatever has been stolen. But, for many companies, the loss of face, the PR loss, reporting an attack is worse than the actual damage. If you are a bank and you have been hacked for a couple million dollars, you are likely to want to keep it quiet. Why scare your customers?

Mr. PALLER. Bruce, let me say something. I have testified here and in the Senate about this issue, can we get companies to report? If we get rid of the Freedom of Information Act exclusion, can we get them to report?

The answer is, "Hell no," but we were unable to prove that until Congress got rid of the exclusion and then found out companies still are not reporting. Now, we know that getting rid of the FOIA problem wasn't enough. But there is a way you can get them to report, and the analogy is medical. In medical reporting, people who get a disease don't call up CDC and say, "I have got a disease." They don't want to. It is just what Bruce was talking about, "It is embarrassing. I am not going to tell anybody." The doctors tell; the patient doesn't

I couldn't figure out for the longest time, but I recently discovered there are doctors in this field. They go into companies right after they are attacked and they clean up the mess under these contracts that are this long on confidentiality clauses spelling out who you won't tell about our being attacked.

You guys are funding a big project at DHS called CWIN, the Cyber Warning Information Network, and you are giving free access to that system, to those "doctors." I think there could be a quid pro quo for their right to get access to CWIN; if you are a doctor and you are helping somebody, you don't have to tell DHS who you are helping, but you must tell the specifics of the attack, so DHS can see if it is hitting anybody else. I think you have that lever right now, meaning these months, and it might actually help.

Mr. SCHNEIER. That is a great example of aligning the business processes to meet our technological needs, because companies don't want to report. And this will work. I mean, that is a great example. Here you can use your buying power. You can use your financial stick to get the data we need.

We need the data. I mean, all the data we have just plain stinks. We don't know how often attacks happen. It is all anecdotal.

In my testimony, I gave three pieces of data, I gave my data and two other pieces of data. They are all mediocre, because companies don't report.

This is very much like the beginning of the AIDS crisis. We didn't know, or the beginning of SARS in China, things were just not being reported.

There is a lot of success. The FBI has gotten way better. You look 4 or 5 years ago, they were completely clueless. Now, they are getting much better. It is attackers that make stupid mistakes. We tend not to find either the attackers that are good and just plain vicious.

You only attack criminals. Criminals, there has to be some kind of financial pay off. There have been cases in England of extortion where the criminals were caught during the money handoff. Criminals are dumb.

When you sort of ask the levels of the attackers, you have the smart attackers who aren't criminals, they are like Mafia Boy, just a bad kid. You have the criminals who tend not to be the good hackers, they are using somebody else's tools.

The real worries are going to be when you start combining these things, right, the sort of quintessential criminal mastermind. These people are sort of rare, because if you are a mastermind, you tend to make more money in the private sector than you do in the criminal sector.

But when you go to places like Russia, where you can actually make good money in the criminal sector if you are smart, there is a worry. Of course, on the Internet, every place is next door to every place else. If you own a warehouse in Des Moines, you just have to worry about criminals for whom driving to Des Moines is a reasonable commute. If you have a network in Des Moines, you have to worry about everybody on the planet. That is big difference. I forget who, someone talked about that. But that is an important difference.

Mr. SESSIONS. I thank the gentleman.

Mr. THORNBERRY. Does the distinguished ranking member wish to ask questions at this time?

Mr. Turner. Thank you, Mr. Chairman. Our primary responsibility as a committee is to have oversight over the new Department of Homeland Security. As each of you know, the new department

inherited the functions that previously came from a lot of other places. In the area of cyber security, we know that the National Infrastructure Protection Center at the FBI was transferred to the new Department, as was the Critical Infrastructure Assurance Office of the Department of Commerce, the Federal Computer Incident Response Center from the General Services Administration, and the National Communications System from the Department of Defense.

When that transfer occurred, we had several things happen. One of which is, it appears to me, we lost some expertise, because the top-ranking individuals who were considered to be very capable in the cyber security area left the government.

We also noticed that the budgets of the cybersecurity agencies transferred to the Department in fiscal year 2003 totalled $180 million. According to the OMB, the current budget for the transferred functions within the Department will drop to about $55 million.

In essence, the new cybersecurity responsibilities within the Department, within the newly created Cyber Security Division, will have in the neighborhood of 60 full-time employees.

When you look at, as each of you I know do, from the outside, from the perspective of the private sector, the nonprofit community, and universities, at what this new department is currently doing to carry out the functions that it has been given to evaluate the threat through cyberspace and to assess our vulnerabilities and to prepare to defend against those threats, it would be easy to conclude that we are worse off today than we were a year ago before the new Department was created.

As observers of that new Department and the cybersecurity functions which have been merged within that Department, I would like to know how each of you would grade the current status of the new Department in dealing with cyber security as compared to the way things were handled by the government prior to the creation of the Department and the transfer of cybersecurity responsibilities to it. I will start with Mr. Paller.

Mr. PALLER. A tough question. All right. The answer in my mind is that no organization will be able to have all the expertise within itself, and some of the money that was lost in forming DHS is still being spent on cybersecurity. There is an extraordinary team at the FBI of cybersecurity analysts. There are some phenomenal cybersecurity people at the NSA. If the new Department gets itself organized and builds the trust of those people in other agencies, and it is the public-facing part of a coordinated government-wide effort, it will be wonderful. But if you try to build the entire capability inside DHS, I think it will just take so long that it won't do enough good soon enough to be effective.

So I guess my attitude is that we may be spending too little, but the way to find out is give them a lot of energy and a lot of visibility and get them moving fast and allow them to show what they can do with that money. Let them show us they can do so much good with that money that we should double or triple it, rather than saying right now we are not giving them enough. They are just people there and only have so many hours in the day.

Mr. PETHIA. From my perspective, I think it is a positive step to bring some of these functions together, because I think in the past they had a tendency to each go off in their separate direction, and there wasn't as much coordination and synergy and impact as there could have been. Having these groups together, I think, is a very positive thing. I am concerned about the budget level. I think it is a big job and there is a lot of work to do there. I know an awful lot of desire is to have folks rely on the private sector to make a lot of changes, but I think it is going to need a lot of coordination and oversight.

I think the real thing to consider as we look at the department in fixing this problem is going to be something we are going to work at for years. This is not a sprint, it is a marathon. Having them have the time to get the right foundations and structures in place, build their relationships with the rest of the Federal Government and the private sector, I think that is the critical thing for them to do right now. Then, as that foundation is built, understand where to intelligently spend money for high impact is the next step. I hope that is what we will see next.

Mr. SCHNEIER. I actually wrote an essay really answering your question a few months ago. With the Chairman's permission, I will send it in afterwards.

Nix, is my answer. My intuition is that security can't be the purview of one organization. It has to be diffuse. If you sort of think about your body fighting disease, there is no one organ in charge of disease fighting. There are lots of different things done by lots of different organs in your body. A lot of them overlap. This are redundancies. All of these things help our body's security against disease.

I actually like it when multiple organizations are working on the same thing, because they are going to work on it differently. I like it when security is the responsibility of everybody, because everybody will do something. I don't like it when Department X can say well, security, that is Homeland's purview. We don't care.

On the other hand, coordination is essential. You need to be able to work together, because a lot of these problems are bigger than any organization.

So I like it when the Department of Homeland Security coordinates. I like it less when they subsume. The real answer is a little more complicated than that, and I will send it in for the record, but that is my intuition.

There is good and bad here. The loss of funding is a perfect example of bad. There are actually few corporate mergers that work out well also. These sorts of things are common when corporations merge. We are seeing the same sorts of things with DHS. Eventually, it could be a good thing, it could be a bad thing. Right now, it is very mixed.

Mr. TURNER. Thank you.

Mr. THORNBERRY. The gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman. I would like to ask unanimous consent that my opening statement be submitted into the record.

I thank the panelists very much for their insight. I will be brief with respect to the issues of this committee because I have listened closely for the time that I was here. I apologize for my delay. I had responsibilities elsewhere in the Congress.

I simply want to acknowledge that we have had the opportunity to be in field hearings across the country and have heard from those individuals who have to fight these issues directly with respect to port security and other issues and law enforcement who are on the ground, if you will. And the key statement that they make is how much is on the Internet, the Web, the voluminous information.

I recall right after the 1995, I believe, bombing in Oklahoma City, that all of a sudden it seemed to be in vogue on how to make bombs with fertilizer. As a Member of the House Judiciary Committee, it is likewise equally amazing at the number of recipes for creative drug use that can be found.

Then, of course, we go smack against this whole question of the first amendment and the protection of a nonencrypted Web system.

So if I could ask Mr. Schneier to confront this head on, in terms of the backdrop of the constitutional protections, the industries' concern, and the freedom of commerce, I guess, that everything goes. But that means that terrorist cells can communicate, while students are communicating, so terrorist cells are communicating, but it also means signals can be sent and it also means directions in code can be sent.

How do we confront that issue head on? You may have been answering it over and over again, and here we go again.

Mr. SCHNEIER. Actually, what I tend to do because I do get these questions a lot, is I tend to write the answers down, so I don't have to do them much. And I have written about this. It is a very hard question, balancing secrecy and security, because there is a notion that secrecy is somehow equal to security.

You talk about bombmaking tools and drug recipes, I assure you, those things were available before the Internet, and you really can't bottle them up. And you are right in that, you know, all tools of our technology can be used for good and for ill. I mean, we drive to work and criminals use cars as get away vehicles. You know, demolitions have good and bad uses. Cell phones have good and bad uses. Even network security products have good and bad uses, and we are stuck with that. That is the way the world works.

Everything we have ever built has uses for good and bad, and we as a society have to decide. We can live in a totalitarian regime and decide no one should have access to a photocopier or mimeograph, which was true in some countries in Eastern Europe. Or we can say the good uses outweigh the bad uses.

I went to the Washington Monument yesterday because I got in a little early. I wanted to go up and see it since it was redone. I was looking at the security. You know something? We would have a better job securing it, if we didn't let people inside. It would be more secure. But we believe that letting people tour our national monuments is a worthy thing to do, and we are accepting the security risk.

Ms. JACKSON-LEE. Let me just say this. You are making what can be a creative analogy, but we have put in place since 9/11 more

structures, more security, more metal detectors, more procedures in going on airplanes, et cetera.

What I would say to you is we are going to have to contend with this question of cyber security. We are going to have to be more responsible. I am a person that believes totally in the 1st amendment and all of its yeas and nays, all of the positives and negatives. But I do believe cyber security is an enormous challenge.

For example, as one of our witnesses in one of our hearings indicated, the economic collapse that could come about through the tinkering why our financial system could be dastardly in its results. Certainly loss of life, the emotion of loss of life, the absolute repugnant concept that we would lose lives in a terrorist act, certainly supersedes the thought as it relates to an economic collapse, but that still would shut us down.

I guess what I am putting on the record is we have enormous challenges. If you have some suggestion or direction, I would be interested in it. I would be delighted if you would put that in writing for us to be able to handle that. If you have one sentence on that response, then I yield back my time.

Mr. SCHNEIER. The problem with secrecy is it is brittle. When you lose secrecy, you lose all securities. I prefer security measures that are resilient. If my front door is protected by a secret code, if someone knows the code, I have no security. If my front is protected by a guard and alarm, then there is more resilience. There is no secrecy that I am relying on for my security.

That is the intuition in the relationship between secrecy and security. Sometimes it is valuable. Most of the time, I believe it is a red herring. Openness is better. We need security in addition.

Ms. JACKSON-LEE. I see the red light. I just want to say this: With all of my passion and commitment for the 1st amendment, I believe that this committee and the Department of Homeland Security has a moral and dictated obligation to deal with the question of cyber security, and we have got to confront it. I hope we will have the experts to help us do so.

Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentlewoman.

It seems to me that all of you are pretty much in agreement that attacks are getting worse and attacks are getting easier and that we could do a lot to deal with 80 percent of these attacks, say, relatively easily, and then we are better able to concentrate on the more sophisticated ones.

I want to be clear. What is it that is required to solve the 80 percent? We have talked some about incentives, liability, maybe taxes. Some people have talked about SEC disclosures and other kinds ever incentives for private companies. Or is it incentives for the software, ISP's and so forth that have been talked about?

Just so I can be clear, first, how do we take care of the 80 percent?

Mr. PETHIA. Let me start. For me, the first big piece is to take care of the, let me call them low-level defects in our information technologies. It can be done by vendors doing a better job of design and testing. The software engineering community knows how to do a better job of that. We know how not to get these kinds of bugs embedded in our software. People can be trained to do develop-

ment, where they don't produce as many mistakes. We can do it with more concentrated testing. We can do it with testing labs that are established to find these problems before they are deployed out into the broad community, or even after things are deployed, to find them. And vendors do respond to reported problems. They do fix them when you bring them to their attention.

So, first of all, I think we have to pay attention to the installed base of software, and there is a variety of different approaches to do that.

The second thing is I think we need to do a better job, all of us, of working together. We have been talking about information sharing for a large number of years, but as Bruce said, it is often catch-as-catch-can; it is haphazard; it is anecdotal information.

We needed to build a national system of data collection, analysis, indications and warnings, so we can begin to understand of all these things we see, which ones are serious and which ones are noise in the system. I think that is a combination of a research effort, but it also requires that organizations that run major networks do a better job of monitoring them.

I think we start to touch on privacy issues when we get into that world. So we need to look at that balance between privacy and the need to understand what is happening to us. So there a set of policies and research questions there.

But I think those two things alone can get us to the 80 percent solution. And I don't think it is tens of years, I think it is years, not tens of years, to do that.

Mr. THORNBERRY. Anyone else wish to address that?

Mr. PALLER. Mr. Chairman, we can fix two sets of problems. One is the vulnerabilities in machines that will be installed starting tomorrow, and the other is the vulnerabilities in the 150 million machines that are already there.

What Rich is talking about is looking at the machines that are going to be installed sometime after tomorrow. So we really have to go after both of those sets of problems.

For the new machines, we either use regulation, as Bruce would like us to do, or liability, or we make the market solve the problem, and that is what I think Homeland Security can do.

Homeland Security can lead the Federal Government in creating the procurement specifications that say, "You can't sell us a system that has these certain vulnerabilities in it. We know what they are. You just have to sign this statement saying you have taken them out or you can't deliver the system." That would change the economics of the problem, and they will start delivering safer systems. That helps with the forward-looking machines, the ones that get installed after you write that specification.

To go backwards to the installed base, I think we could take a lesson from the Department of Transportation. DOT has done an extraordinary job of wiping out vulnerabilities across the Department. I think DHS can learn from the agencies that have been successful. Homeland Security can be the model, and I think that model will spread. But we need to do both and go after new machines using procurement, and go after the old machines using vulnerability remediation.

I need to add one more piece. People are building hardware with vulnerabilities, and you are buying them right now, and when you move to wireless, you are goint to see vulnerabilities in billions of devices. Every one of those devices can be used as an attack tool. So this isn't something we need to spend the next year and a half thinking about. We need to act now.

I will give you an example. Every one of your storage devices, where you put your most important information, has something called IP management ports. The ports were put in for the convenience of the guy who sold the storage system to you so he can help you fix it if it breaks.

Some of those IP ports come with known vulnerabilities, SANS and the FBI publish every year the top 20 Internet vulnerabilities. Storage devices come with many of these top 20 built into the hardware.

Your procurement people are continuing to buy that stuff, because the people who buy it don't know it has common vulnerabilities. That needs visibility. Homeland Security should be taking the lead on procurement programs, and then helping, maybe through a partnership with the Government Reform Committee, helping other agencies do the same thing.

Mr. THORNBERRY. Let me just throw in another wrinkle for you, Mr. Schneier.

Mr. SCHNEIER. I will take wrinkles.

Mr. THORNBERRY. I was in a meeting last week where a CEO of an information technology company said as bad as we think the security problems are for us with 300 million users on the Internet, whatever it is, think about how much worse it is going to be if that triples. And if you think about wireless, plus the number of additional devices that are going to be using the Internet, plus some natural growth in number of people around the world, that it nearly makes the problem insoluble.

Sometimes I worry, as you all have described, we are getting further and further behind. Maybe we could do all of these things and solve this 80 percent, but there are going to be another 80 percent that takes its place in a way. How do we catch up and stay up?

Mr. SCHNEIER. It sounds like you got it.

Mr. THORNBERRY. But I don't like what I have got.

Mr. SCHNEIER. Well, you know, sorry. A lot of it, the analogy I use is, you know, is curing malaria by draining the swamp. You have got all of this swampland out there. It is horribly insecure, and we are trying to improve security by fixing it. The problem, as you point out, is we are creating swampland at such an alarming rate, that we are falling behind.

Yes, you are right. You are 100 percent right. The thing about these easy fixes, I mean the things we are talking about here, is they are actually easy. It is not things we discovered 2 years ago that need to be fixed. It is things we discovered 20, 30, 40 years ago and no one has fixed.

The most common attack is something called a buffer overflow. It doesn't matter what it is. These were first identified in the sixties. They were first used to attack computers in the seventies. There was a very famous attack in 1989, which was a buffer overflow.

So here we are in 2003, and, still, the most common Internet attack is a buffer overflow. This is an easy one. We know how to fix this. This is trivial to fix. These guys will teach classes in how to write code buffer overflows. This isn't even a hard problem.

So yes, we are creating new swampland, but the problems we are talking about here are so basic, they have been with us since the beginning of computing, and there has never been the business incentive to make them better. So once you do that, there will be a change.

You are right, there will always be new vulnerabilities. We raise the bar, the bad guys will get smarter, guaranteed. But at least the ones who are not smarter, are out of business. We are better off than we were.

So we are not here with a message of hope. We are here with a message of we can actually do better than we are doing.

Mr. THORNBERRY. Good point. Practicality. The alternative is to do nothing, which is to accept the vulnerabilities, and that is not a good answer either.

Take the 80 percent. Let's talk for a second about the other 20 percent. Do any of you have suggestions as to the way Federal research dollars and efforts ought to be directed to help deal with that 20 percent?

Mr. SCHNEIER. I can do that. Actually, you go. We'll flip for it.

Mr. PETHIA. Let me start. We have been talking a lot about sort of sticks we can use to encourage the right kind of behavior, but I think there are incentives as well.

The Internet today is a result of the original DARPA projects, the ARPA net, which was focused on building a resilient network that could withstand physical attack. And it has done that job amazingly well. It has grown into this new infrastructure, it has created a whole new industry.

I think we can do the same with security, if we think about not Internet II, but maybe Internet III or Internet IV, where the focus is not on resiliency from physical attack, or it is not on what, as Internet II is, on higher speeds, let's have the next grand project be focused on the ultimate high security.

I think that mobilizes the research community, the industrial base, and they all begun to work on this new common set of solutions, which is technologies that are significantly more secure than the things we have today, from the beginning, security that is designed in, as opposed to what we do today, which is try to bolt it on to the outside edges of fundamentally insecure projects.

Mr. SCHNEIER. I like to see research money spent willy-nilly. I think the most best research, the most interesting things, come out of the most surprising places. Because I write books and give lectures, I get a whole lot of people's term papers, and there is really cool stuff being done out there. Some of it is so interesting it never would have occurred to me.

If we are going to fund research, now we are talking about many years ahead, we need to be broad. We need to recognize that this is a critical area of our society and that we need to fund research programs at a variety of institutions, maybe even internationally. There is great things being done in Europe and Asia. This problem is even bigger than our country. It is all the same Internet.

I love the idea of procurement and research on a secure survival Internet. That is how we got the Internet. That is how we will get a secure Net that is great.

And then keep in mind that we should just fund research institutions, universities, that are doing cutting edge work in computer security. Whether it is producing secure hardware and software, like the computers we are going to install tomorrow, or backfilling and securing the computers we installed yesterday.

Research is good. Great stuff comes out of research. I love it when I see it, because it is creative, it is interesting, and it is looking at things that are off the horizon.

So I encourage lots of research, because you never know what is going to bear fruit.

Mr. THORNBERRY. Mr. Paller, I would like to ask you to answer however you like and throw in another wrinkle, and, I don't know how to say this, but do we need research on some of the cultural aspects of security, whether people on a keyboard are really going to do it, use it? How does that play in to making the whole Internet secure? The people vulnerability, I guess, is the way I would put it?

Mr. PALLER. It is really no fun to try to finish the job of figuring out how to do the technical security work when you know that having finished that, you still have an enormous vulnerability from people taking their laptop home, giving it to their 11-year-old, who downloads a really, really cool screensaver that has a trojan in it that the hackers use to get right back into the House systems, because you have a VPN that runs from your laptop at home into the system in the House. We know that is a problem. I would love to see research in solving it.

My sense is that it is a safe driving type of problem, meaning it requires a long-term cultural change. This afternoon, for example, Bob Liskowsky and I are giving out awards to 10 kids from kindergarten to high school all over the USA who created posters on improving computer security.

It is a tiny drop in a huge ocean, but a long time from now we hope kids will talk about safe computing at home the way they get mad at their parents for not wearing their seatbelts. It took a long time for kids to tell their parents to put their seat belts on. I think research will help. I think visibility like this subcommittee provides will help. It is a long-term program.

Mr. THORNBERRY. I guess the question is how much pain we have to go through or how many people have to go through the windshield before we do it.

Mr. SCHNEIER. A lot.

Mr. THORNBERRY. Does the gentleman from Texas have other questions?

Mr. SESSIONS. Yes, I do, Mr. Chairman. Thank you so much.

One of you gentleman has already accused our Chairman of "getting it," probably you, Bruce.

Mr. SCHNEIER. I probably did.

Mr. SESSIONS. My question is, I have heard you allude to the FBI as being perhaps short of being a center of excellence, but you did accuse them of stepping up, understanding. Let me tee it up. Fighting city hall is hard. They are the experts. They know everything.

They are the ones that set the standard and tell you stop or go or maybe so. You never really get a lot of answers out of them.

Does our government, outside of this great subcommittee, the government, the agencies, do they get it? Do they listen to people? Do they respond? Or are they just at limitations with money or other things? Do they get it?

I am talking about the computer security experts in these agencies sharing information, talking with you, being leading edge, knowing what is wrong, aiming at the problem, talking about things, leading to where our children understand it, all those things.

Mr. SCHNEIER. The computer security experts get it. We have any number of customers in local and Federal Governments. Uniformly, computer security experts either in governments or industries get it. The problem they have is going one level above them, convincing their boss, convincing the CEO, convincing whatever the legislature is that is appropriating funds.

The security people always get it. I mean, they know the problems, they understand it. It is one level above that we have the problems at.

This is where you find that people tend not to get it. Either they downplay the risks, or they overreact. We have seen, I forget the State, but some kid hacked into a school computer and changed grades, and he is being tried as an adult. To me that is huge overreaction. I mean, changing grades is an enormously big thing and should be dealt with as you would deal with that, maybe expulsion, but he is still just a kid, he is a dumb kid. You don't want to destroy their life by making them a felon.

So you need to temper. Even our prosecution, it has to be sane. I see a lot of what I think is insane prosecutions because we are overreacting.

I am reminded of the Wild West, when stealing a horse was punishable by hanging, because that was such an enormous part of the Wild West transportation infrastructure that the punishment exceeded the crime. We are seeing that again here.

So, you know, I see "don't get it" at different levels. I see it at the level above the computer security people, the Governors, the Mayors, who tend to downplay the risks, just like corporate bosses do. And then I also see the prosecutors either, Federal or State, basically going to lynch kids.

I think both are bad. How is that for inflammatory?

Mr. PETHIA. I would like to build on that. One of the things I think is very positive in the government right now is the whole list of regulations moving now to FISMA, and I think it has done a lot to have senior executives in the agencies begin to understand that there is a problem there.

What I see though is we are starting to get stuck at the point where people are worried about compliance with regulations or compliance with standards, which says they are not quite far enough up that learning curve as we have to do.

The thing to remember about computer security is it is a daily event. It is not just complying with a standard or a regulation, it is day-to-day having the awareness, to keep your eyes open, to

watch for that strange thing that is some indicator that your systems are being compromised.

So there I think we have to help the senior officials push up that next step, beyond compliance regulation, with a real understanding of there are critical assets that have to be protected, they can be attacked in a number of different ways, and everybody has to be trained, aware and vigilant.

Mr. PALLER. Let's bring these all back together. Yes, we have to persuade them in. But right now, when they get an expert in that expert comes with a price tag that is enormous, and when they ask, "Is that enough?", the expert will say "No!" So you have a meeting with a guy who says, "Spend $50 million, but it won't keep your system safe." And you say come back to me when you get a clue.

There are good models in governments. Congressman Smith was getting at it when he said we have to make security cheaper. People in government are figuring out how to lower the cost of security, and that is where we are going with using procurement to push vendors. The vendor push is not to put the costs on the vendor, the user still has to pay for it. The vendor push is to get the economies of scale that you get when the vendor does initial security instead of making every user do it.

DOE's procurement is not trying to force Oracle out of business. It is saying, "Look, Oracle, if you deliver safe systems, every one of the Energy labs can get those safe systems, instead of making every Energy user become a security expert before he ever installs the software."

I think that the other discussions we were having about pushing it back on the vendor to getting safer systems, allows senior management to say, "OK, I can see that working, let's do that, let's get those vulnerabilities eliminated." And, in fact, FISMA requires the agencies actually test their systems. That is what I meant by going back over the old systems and making sure the security controls are in place. I think there is reason for hope. I don't think we will win the war, but I think there is reason for hope.

Mr. SESSIONS. I have one last question. I have not participated in it, but evidently Microsoft, the way I understand it, they have an open chat page about all their products, the design problems, and all these millions of users e-mail in.

Mr. SCHNEIER. It sounds plausible.

Mr. SESSIONS. Somebody evidently designs a system where they take user input and they fix things, and they have the user community try to provide input about fixing software programs.

My question is, in all these chat rooms and all this feedback that comes from people, do they understand that if you are going to use this equipment that there is an ethics about it, or do they just think, hey, what I would say a skateboarder, whoever can do the next wild thing, go for it, and everybody sits there and applauds? Or is there an ethos within at all that is ever applied to these people?

Mr. PALLER. I have never seen an ethos. There was a survey done in Australia of how many kids in the 12th and 13th grades were breaking into other people's computers 4 years ago, and it was 3.2 percent of all the males. I don't think there is any ethos being taught.

Mr. SCHNEIER. But we should take heart in that. Most people are ethical. Most people are honest. The great majority of people on our planet are honest. That is why society works. We would just fall apart if that were not true. We are dealing with the few. I mean, three percent is still three percent. Cutting that down by a tenth would be really good.

This is how we eventually win, I believe. Sort of imagine we are having this hearing about murder and how do we deal with murder? It is happening. I mean, there are no technological fixes. What do we do?

All right, we don't prevent murder in our society by wearing body armor. We don't drive tanks, we don't live in fortresses. The reason murder is so low is that we have carrots and sticks. We teach ethics. We expect our children to behave ethically. We reward them if they do, and there is a criminal system to punish them if they don't. That is really how we deal with crime.

No one says we think everyone should wear a bulletproof vest walking around the street, no matter how bad the murder rate is. I mean, it is not something we do.

Now, this is very long-term, but in the end I think that is going to be the way out. But you still have to deal with the few, and, of course, the problem on the Net is the magnitude, right? The few can do a whole lot of damage.

Mafia Boy, who we have brought up again and again, can attack dozens of web sites. The guy who wrote the Sequel Slammer Worm can have it spread across the Internet, some huge number of servers, in 15 minutes, in 20 minutes.

So we can, through education, through deterrence, make sure most everyone is ethical. The few that are aren't can do so much damage, either out of maliciousness or even by accident, or out of carelessness, or out of, you know, dumb-kidness, that we need to have these high walls.

There is in the military, I forget who it is, who looks at society, the danger in terms of how many people 10 armed men could kill before being subdued. He will go through history and calculate this. All right, that number is going up exponentially with technology.

The Internet has all the kinds of characteristics of that exponential growth. One guy can do a whole lot of damage. So even if we have everybody ethical on the planet except 10, we are at risk. That is a hard position to be in. It is no fun to be here. This is the ugly side of technology.

Mr. THORNBERRY. But that is where we are, as you said earlier, in all sorts of areas.

I guess I have got one last question, because I don't think it has been touched on, and I am interested, Mr. Pethia, particularly in your perspective, on the kinds of information that government should provide to the private sector about threats that are out there, warnings perhaps, obviously this is part of what this new part of the Department is going to focus on.

But can you address that a little bit, as well as addressing how you have to weigh, how much information about threats you put out there, versus the government's duty, if it has that, to say watch out, this is coming, when, as you have all already described, when

something starts going it goes quickly, and it is going quicker and quicker.

Mr. PETHIA. I guess a couple of points. One of them is certainly, I think, the government, and it has been doing it through my organization and through NIPC and through a number of others, when there are recognized new forms of attack, to make sure that that is broadly and as quickly as possible sent out to the community so they know how to protect themselves. And a lot of that is with the hope people can react fast enough. As you say, these things are happening faster.

One of my big concerns, which is yet another issue, is that we are reaching the limits of our reactive capability, I think nationally. We are all going to get incrementally better, but we have already got the 80 percent. We are already going about as fast as we can.

So we have got to focus more on prevention. We have to look for earlier signs of attack. We have got to look for earlier indicators that something bad is coming at us. And there, I think, DHS ought to look at doing things like looking at the evolution of attack technology, and beginning to predict where it could go in the future, what we are likely to see in 6 months, 8 months, 12 months, what have you, and trying to get that information out to the community.

Real threats, I mean real people doing bad things, getting as much information as they can out to the likely targets of those classes of people, which industries are being attacked and how, so those industries now how to protect themselves.

Mr. THORNBERRY. Does anybody else wish to address that?

That is helpful.

Mr. ANDREWS. Mr. Chairman, if you could yield for a moment, I wanted to express my appreciation to you and the staff, the majority and minority staff and the witnesses, for what I think has been a profoundly important hearing. I very much appreciate what the witnesses have had to say.

What I wanted to suggest to you, Mr. Chairman, is that we consider working with the Government Reform Committee, which has primary jurisdiction over government purchasing, so the kind of purchase-based leverage that we have heard about from each of the three witnesses today, goes beyond what the Department of Homeland Security do, but reaches into every aspect.

Frankly, the Department of Agriculture should be buying software that is as good as it can get for reasons of bioterrorism. The Department of Transportation should be buying software as good as it can get when it deals with issues of oceanography. The Department of Education should be buying software as good as it can get to protect the security of student records.

This not only has benefit in carrying out the missions of those various departments, but it multiplies the leverage that these witnesses have talked about here today, and I think would expedite the process of raising the level of technology.

One thing that Mr. Schneier said that I thought was an interesting analogy was the wireless burglar alarm systems in our homes. I would not have been able to afford a burglar alarm system 15 years ago, they were too expensive. Now, they are relatively inexpensive.

That is the metaphor. I think that is the analogy we could achieve for the civilian sector, so when the CIO of a company hears from his or her outside consultant that you need to spend quite a bit of money to ramp up, it isn't nearly as much money as it is today. It fits those economies of scale.

I think it has been very powerful testimony. I thank you and the staff for an excellent hearing.

Mr. THORNBERRY. I thank the gentleman. I think you make a very good point. I would simply add, I also don't dismiss the Department itself's information technology. I think one of the things that I know is of interest to most members on this subcommittee is how the Department gets its own IT up and running and the security there. We have further work to do there, as well as working with the other departments.

Let me again thank each of our witnesses. I agree it has been very helpful for me. Let me say there may be written questions that may be directed to you. We will try not to over burden you. At the same time, I want to offer each of you the opportunity to submit further comments if you think it would be helpful to us, because most of us do read that stuff, and we are interested in learning and trying to find solutions to these problems. I very much, again, appreciate your time and flexibility in being here today.

Let me, finally, announce that I think this room is going to be used for another hearing of the full Homeland Security immediately after this, and they asked me to ask if we could clear the room so they can get ready for that hearing which begins at 2:00. In the meantime, we have votes on the floor.

This hearing is adjourned.

[Whereupon, at 1:25 p.m., the subcommittee was adjourned.]